DDSI

IST-2000-29202

Work Package 1.2 – Part B

International Organisations and Dependability-related Activities

DRAFT

Report Version:	1.1 FINAL	
Report Preparation Date:	31 May 2002	
Preparation led by:	RAND Europe	
Classification:	Public	
Contract Start Date:	1 June 2001	Duration: 18 months
Project Co-ordinator:	RAND Europe	
Partners:	RAND Europe (NL); King's College London (UK); Cell Network (SWE); IABG (D); Almaweb (IT); LINK (PT); ELIAMEP (GR)	

Project funded by the European Community under the "Information Society Technologies" Programme (1998-2002)

Document Control

This report was written by Leon Cremonini, Ingrid Geesink, Andreas Ligtvoet, Allison Myerson, Neil Robinson, Stephan De Spiegeleire, Liese Vonk (all RAND Europe), Dr Robert Anderson (RAND Santa Monica), and Dr David Mussington (RAND Washington), and was edited and compiled by Dr Kevin A. O'Brien (RAND Europe), with the support of Maarten Botterman (RAND Europe), Dr Andrew Rathmell and Dr Lorenzo Valeri (King's College London). The present volume constitutes Part B of the DDSI deliverable D1.2.

Table of Contents

ASIA-PACIFIC ECONOMIC CO-OPERATION (APEC) 4

INTERNATIONAL BUSINESS AND CONSUMERS' GROUPS 8

COUNCIL OF EUROPE (COE) 19

INTERPOL 32

EUROPOL 36

INTERNATIONAL TELECOMMUNICATIONS UNION (ITU) 39

NORTH ATLANTIC TREATY ORGANISATION (NATO) 46

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD) 54

UNITED NATIONS (UN) 64

WORLD TRADE ORGANISATION (WTO) 75

ASIA-PACIFIC ECONOMIC CO-OPERATION (APEC)

The involvement of this regional organisation in the area of Information Security and Assurance (IS&A) derives from institutional interests in promoting electronic commerce between the US and the Far East.[1] IS&A were not previously considered as main priorities for APEC; however, events surrounding the ILOVEYOU virus (and subsequent attacks such as 'Code Red' and 'Nimda') have changed this.

Socio-Political, Economic, and Commercial Overview

At the 1997 APEC summit in Vancouver, participating leaders and ministers 'recognised the importance of electronic commerce and accorded high priority to identifying ways to maximise its social and economic benefits for all APEC member economies.'

At the end of a ministerial meeting in Kuala Lumpur in 1998, government leaders endorsed a *Blueprint for Electronic Commerce* to encourage both sides of the Pacific to exploit the positive aspects of the Internet and its associated information and network technologies. In this context, an Electronic Steering Group was created in February 1999 with representatives from government and business from both sides of the Pacific. This e-commerce focus was confirmed at the recent APEC Leaders' Meeting in Auckland, New Zealand. On this occasion, ministers encouraged economies to take advantage of the self-assessment tool for electronic commerce, as well as to adopt the provisions indicated by the UNCITRAL *Model Law on Electronic Commerce*. Finally, officials were asked to initiate work on consumer protection, information sharing, and best practices.

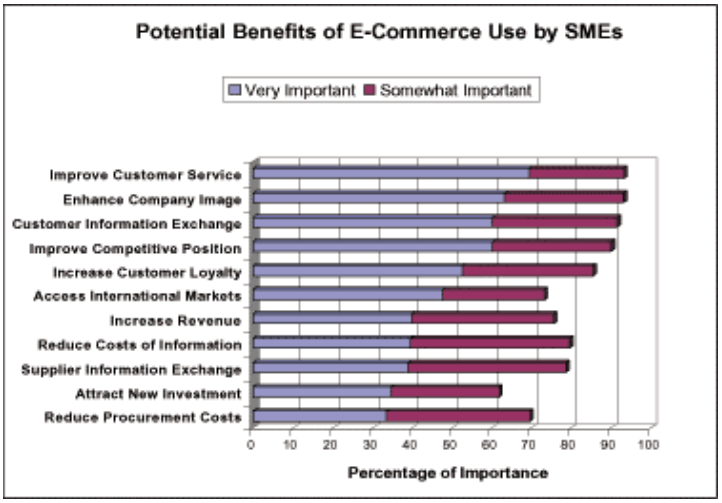
APEC is currently working on issues related to electronic authentication as part of the Telecommunication Working Group. The objective of this group is to foster the 'exchanging, compiling, and disseminating telecommunications infrastructure and regulatory information…and to promote electronic commerce and standards information'. Work on electronic authentication is led by Australia. The activities of this group are still in their infancy, although there is a focus on describing specific technologies and supporting the development and implementation of policies to facilitate interoperability. The Telecommunications Working Group commissioned a survey in September 1999 on the take-up and penetration of e-commerce in the region. PricewaterhouseCoopers conducted the survey on behalf of the working group and asked 3,000 Small- to Medium-sized Enterprises (SMEs) about the of use of electronic commerce. While there were significant positive aspects to take-up identified by countries in the region, the barriers nearly always included security in the top three. SMEs consistently identified that the following were important factors in getting businesses to take up e-commerce: Improve Telecom Infrastructure; Reduce E-Commerce Legal Barriers; Improve Business Access to the Internet; Fair Tax Policy for Transactions; Develop a National E-Commerce Strategy; Raise Business Awareness of E-Commerce; Improve Government Services on the Internet; Enhance Government E-Commerce Use; E-Commerce Training; Promote E-Commerce Use; Provide Web Page Facilities; and Raise Awareness of Y2K.

At its October 2000 meeting in Bali, APEC was urged strongly by the USA to develop a co-ordinated approach to protection of critical information infrastructures. In particular, delegates discussed ways in which IA science and technology collaboration could underpin collaboration in wider areas of IA policy, perhaps even bringing states such as China into the global CIP debate.

---

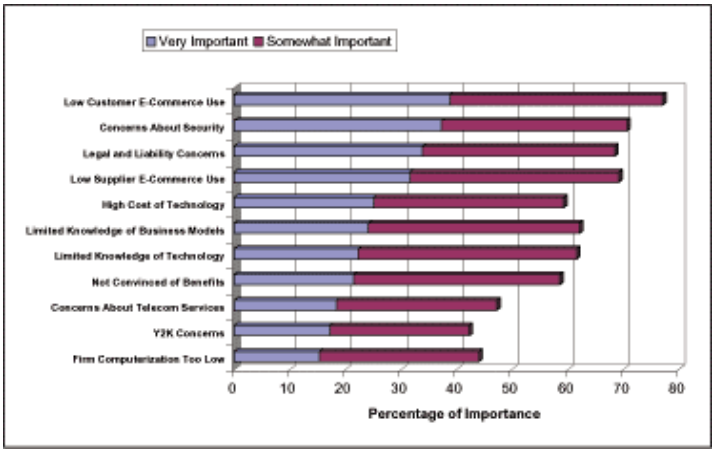
[1] Information collected from www.e-commerce.gov/apec and www1.apecsec.org.sg/workgrup/e-commerce.html (downloaded 1 August 2000).

Barriers identified in the PricewaterhouseCoopers Report prepared for APEC's Telecommunications Working Group's Business Facilitation Steering Group (BFSG) – entitled "SME Electronic Commerce Study" – include: Firm Computerisation Too Low, Y2K Concerns, Concerns About Telecom Services, Not Convinced of Benefits, Limited Knowledge of Technology, Limited Knowledge of Business Models, High Cost of Technology, Low Supplier E-Commerce Use, Legal and Liability Concerns, Concerns About Security, and Low Customer E-Commerce Use.



Source: *PricewaterhouseCoopers Report prepared for Asia Pacific Economic Co-operation's (APEC) Telecommunications Working Group's (TEL) – Business Facilitation Steering Group (BFSG) "SME Electronic Commerce Study" Final Report (24 September 1999): 11.*

APEC work in e-commerce stems from an agenda set up by the Telecommunications and Information Working Group in 1998, which coincided with the creation of the e-Security Task Group. An e-commerce steering group was established in 1999. The goals of APEC's work in this area are to facilitate trade, identify and address impediments, and map developments in individual countries. At the 2001 Senior Officials' Meeting (SOMI) in Beijing, the e-APEC Task Force (eATF) was formally established. The mission of this group is to develop the Action Agenda for the New Economy and ultimately deliver a long-term strategy with definite action points for the development of an ICT-based new economy in the region.



Source: *BFSG "SME Electronic Commerce Study" Final Report: 21.*

Broadly speaking, the three main goals of eAPEC are to strengthen market structures and institutions to take advantage of the new trading environment; develop a policy environment for investment in infrastructure and the development of technology; and finally to improve training, skills, and education to kick start innovation and entrepreneurship.

A legal guide was produced for APEC by the regional offices of Baker and Mackenzie law firm, which should go some way in addressing awareness issues regarding the conduct of ecommerce in the region. The guide seeks to cover industry and governments concerns about rights, responsibilities when using the Internet, and other ICT-related technologies when conducting business online in the APEC region and was specifically focused on SMEs.

Analysis of the Main Regulatory and Legal Developments Related to Information and Telecommunication Systems and Services

APEC, under Australia's leadership as the Chair of the TEL-WG (in particular the Australian National Office of the Information Economy) has conducted a number of extensive surveys of legislation relating to Information and Telecommunications throughout APEC member-nations.

Specification of suggested legal courses of action for member states is contained within the 'e-APEC Strategy', which reaffirmed a decision made at Brunei to build a digital society within the APEC region. Legal and legislative provisions are to spur the development of productivity, stimulate economic growth, increase employment opportunities, upgrade public services, and improve quality of life by taking advantage of advantage of advanced, reliable, and secure information and communications technology (ICT) and networks by promoting universal access.

A stated goal is reducing or eliminating the requirement for mandated paper-based documents in cross-border trade within the region. APEC is looking to push for the removal of a number of regulatory and institutional requirements for paper-based documentation which, it hopes, will improve efficiencies in the manufacturing economies of member-states.

A key finding has been that governments with strong cross–agency co-ordination mechanisms already in place are likely to be the most successful in the removal of these barriers. Challenges identified include the take-up of laws supporting electronic transactions, the removal or alteration of laws requiring paper documentation (e.g., paper- vs. electronic signature-based arguments), and IT investment and complexity of the provision of online public sector trade services (e.g., export regulations).

Assessment of Phenomena Undermining Dependability

APEC's assessment of threats to information infrastructures and the take-up of e-commerce is that serious accidents and natural disasters will continue to occur. This recognises the importance of contingency planning in the operational day-to-day management of business generally, whether this be conducted exclusively via online methods or not. Secondly, the organisation recognises that a new set of threats to the regional critical infrastructure will appear, and that many of these threats will have a cyber dimension. Judging by its use of the term critical infrastructures, APEC has taken notice of US pressure to accept the existence of these sorts of infrastructure. APEC also recognises that networks, while being increasingly powerful for the provision of commercial and governmental services, are also vulnerable to threats of a predictable or non-predictable nature (e.g., natural disasters) or low-–risk/high--impact events. The high incidence of natural disasters in the region, coupled with the concentration of populations, infrastructure, and wealth into small, highly-developed areas and the reliance upon dated infrastructure are all stated problems for the development of dependable ICT networks, and the take-up of electronic services.

APEC also recognises that old threats and problems are taking on new faces, and that ICT networks are altering the structure of old threats (crime, terrorism, espionage) as well as being the focus for new types of crime (web vandalism, 'hacktivism', among others).

Organisational Initiatives Aimed at Tackling Cyber-Security/Cyber-Crime or Assisting with the Development of Dependability

APEC's Electronic Commerce Steering Group has been conducting work on methods of authentication. ECSG has primarily been looking at how technology-neutral solutions can be identified for authentication in e-commerce. A diverse program of study has been set up, which has involved the private sector to a large extent.

APEC is looking to work on a number of areas related to tackling the issue of poor electronic security and dependability. Such measures include identification of business requirements, promotion of IT standards and models, ethics packages for IT security, the consideration of the effectiveness of broad guidelines (self-regulation) rather than imposed measures, and finally identification of challenges. Specifically, APEC puts forward that there is a need for co-operation in international fora, awareness-raising, and the exchange of information relating to CIP (although it may be interesting to see how many nations in the APEC area are aware of definitional issues relating to CIP and the CNII). APEC also suggests that the provision of examples (good practice) may be a useful way of promoting what it calls 'reliable information transmission'.

In 1997, at the 15th meeting of the Telecommunications Working Group, it was decided to establish a task group on Public Key Authentication. However, this was later changed to Electronic Authentication to reflect the diversity of electronic authentication methods.

The e-Security Task Group has completed work on information infrastructure protection and many broader e-security issues. Australia, New Zealand, and Japan all submitted reports concerning national CIP initiatives, so awareness of work in this area is growing.

The Telecommunications and Information Working Group is proceeding apace with its 'Cross–Country Smart Card-Based Secure Electronic Commerce' project, whose remit is to investigate the system and security aspects of secure electronic commerce in the region. The project has as its deliverables a technical paper on the design of a cross-country PKI (Public Key Infrastructure). The design is particularly looking at the effectiveness of smart-card solutions to e-commerce security issues. TIWG is also producing a survey on secure e-commerce in the APEC area of interest. Both of these projects are in support of the Asia Pacific Information Infrastructure Initiative (APIII).

INTERNATIONAL BUSINESS AND CONSUMERS' GROUPS

International Chamber of Commerce (ICC)

Headquartered in Paris and founded in 1919, the International Chamber of Commerce (ICC) is the leading global business organisation, whose objective is to promote an open international trade and investment system and the market economy.

Today, ICC groups thousands of member-companies and associations from over 130 countries. Because its member-companies and associations are themselves engaged in international business, ICC claims to have unrivalled authority in making rules that govern the conduct of business across borders. Although these rules are voluntary, they are observed in countless transactions every day and have become part of the fabric of international trade.

ICC initiatives are directed at issues of trade and investment policy, as well as vital technical and sectoral subjects. These include financial services, information technologies, telecommunications, marketing ethics, the environment, transportation, competition law, and intellectual property, among others.[1]

About a decade ago, ICC started to focus more on specific issues related to electronic commerce, such as information security and computer crime. In 1998, ICC released a set of model clauses for use in contracts involving the global transfer of data. The goal of this initiative was to provide international businesses with specific guidelines in order to reduce costs, while satisfying the requirements of the various national data protection authorities. Similarly, a set of guidelines regarding digital signatures was released in order to facilitate the exchanges of online contracts among international commercial partners.[2]

With the number of computers linked to the Internet growing at a spectacular rate, the business community has become increasingly concerned at the prospect of a corresponding explosion in crime involving information systems and the Internet. In response to these concerns, and to meet growing demand from the ICC's worldwide membership, in the second half of 1999, a new unit was set up. The Cyber-crime Unit is part of ICC Commercial Crime Services (CCS), the London-based specialist arm of the International Chamber of Commerce that focuses on crime in the business world. The unit provides operational support to the three specialised bureaux of the CCS - the International Maritime Bureau, the Commercial Crime Bureau, and the Counterfeiting Intelligence Bureau.

Specific Cyber-crime Unit tasks are to:

- keep track of criminal methods and brief CCS members;
- provide expert advice on security of information systems;
- identify criminal interference in corporate computer networks;
- constitute a prime source of information, research, and intelligence; and

---

[1] www.iccwbo.org

[2] Andrew Rathmell and Kevin A O'Brien, *Information Operations: An International Perspective* – Special Report. Jane's Information Group (December 2000).

- work closely with national and international law enforcement agencies.

Thus, the ICC Cyber-crime Unit helps businesses in the prevention of criminal activity through technical assistance and consultancy, offers post-crime investigation and advice services, and acts as an interface between law enforcement and the private sector.

Confidential information packages should keep ICC members abreast of developments in the area of computer crime. Co-operation agreements have also been established: the Cyber-crime Unit holds regular consultations with senior international police officers (for example, the Unit works closely with Interpol to tackle internet crime on an international level) and is a conduit for exchanges between law enforcement and business.[3]

In January 2000, the Cyber-crime Unit presented its anonymous reporting service for companies who have been victims of criminal activity on the Internet, and whose experiences could prevent other e-businesses falling prey to similar attacks.

Businesses may sometimes be reluctant to report Internet crime incidents for fear of bad publicity or commercial espionage. The service means that companies that have been victims of Internet crime will be able to describe the nature and details of the offence without divulging their name, so that others may take appropriate precautions.

However, also getting information over to its members about which Internet crimes they need to protect themselves from is one of the main aims of the Cyber-crime Unit. 'Although business is aware that Internet crime is a problem, much of the general information available on how to prevent it may be over-technical or not relevant for an individual company's particular system or products,' according to Captain Pottengal Mukundan, Director of ICC Commercial Crime Services.

ICC members do not have to trawl through numerous information sources and filter out everything that is not relevant to their products, as the CCU will do this for them, providing a 'one-stop' shop for all the products that they use to maintain a secure web presence. Furthermore, members will not have to go looking for the information, as the CCU will send it directly, via (secure?) email as soon as the data have been collated.[4]

Related to this service is the 1999 cyber-crime survey where businesses can report any Internet-related attacks or crimes suffered in the last year. To get more insight into the scope of the computer crime problem, ICC asked its members to report, among others, the attack type (Trojan horse, packet sniffing, denial of service, spoofing, access control, session hijacking, DNS hijacking, intrusion due to a design vulnerability, virus, or other); the result of the attack (website vandalism, lawsuit, loss of confidential information, loss of data, damage to reputation, disruption of operations, etc.); and several technical details of the system.[5]

Other activities of the Cyber-crime Unit include courses, like the workshop for business on managing the cyber-crime threat, held from 20 -25 May 2001 in Norfolk. During this interactive course, businesses explored their areas of vulnerability and found ways to protect themselves.

---

[3] More info on ICC Cyber-crime Unit can be found at: www.iccwbo.org/ccs/menu_cyber-crime_unit.asp. See also: Rathmell and O'Brien, *Information Operations: An International Perspective.*

[4] ICC: "Cyber-crime bulletin urges victims to share information". London (12 January 2000): available at: www.iccwbo.org

[5] For the 1999 Cyber-crime survey: www.iccwbo.org/ccs/news_archives/2000/first_cyber-crime_bulletin_survey.asp

Finally, the ICC is also developing specific initiatives aimed at fostering 'electronic trust' among potential e-commerce business partners. In August 2000, the eBizID programme was launched. This initiative, managed by the Hong Kong-based company ITradeSecure, is a secure digital identification solution based on public key infrastructure (PKI) and is composed of distinct elements. First, there is a Common Corporate Identifier containing a specific set of company information. Second, there is an EBizID Trust mark that verifies the fact that the holder has gone through a comprehensive verification and authentication process. Finally, digital certification and signatures, as well as encrypted email and enterprise-wide PKIs, are provided to allow companies to trade securely over the Internet. In order to deliver a full solution, the EbizID programme has partnered with companies such as IBM and its subsidiary Tivoli, Qualsys, Coface Rating, and SGSonSite.[6]

The Internet Alliance (IA)

The Internet Alliance (IA) is an organisation of Internet policy professionals. As one of the leading international business advocacy organisations, and headquartered in Washington, DC, IA represents the Internet online industry at the state, federal, and international levels. Through public policy, advocacy and strategic alliances, the IA aims to build the confidence and trust necessary for the Internet to be the global mass market medium of the 21st century.

Members of the Internet Alliance include IBM, Bell Atlantic, @Once, 24/7Media, AOL Time Warner, Citibank, Encirq, Cox Interactive, Deutsche Telekom, DLJDirect, MCI WorldCom/UUNET, Council of Better Business Bureaus, Microsoft, Prodigy, Juno On-line Services, WorldCom, Verizon, and Yuroka. The alliance is an independent subsidiary of the Direct Marketing Association (DMA).

Having formed strategic alliances within the Internet policy community, the IA is dedicated to advocating the Internet industry's perspective on issues such as online consumer privacy, Internet security and law enforcement, content regulation, unsolicited commercial e-mail or 'spamming', internet taxation, and children's marketing online.

The Alliance is also dedicated to coalition- and alliance-building by co-operating with other reputable associations and public policy organisations to strengthen further the industry's voice. Besides effective partnerships, IA's mission statement is to persuade governments of the need for the Internet's self-governance. Firmly committed to the notion that the Internet cannot support a 'Balkanised regulatory environment', the IA argues that 'self-governance is critical to the survival and long-term growth of the medium and the Internet industry as a whole'.[7]

Against the background of a growing threat of criminal activity online, the IA aims to serve as a pragmatic industry voice by co-ordinating industry initiatives on education outreach to policymakers, law enforcement, and consumers. The IA's goal on this issue is to lead industry self-governance discussions, memorialise a critical set of business practices to help thwart crime, and demonstrate the industry's continued commitment to stopping crime and fraud online**.**

Information security and computer crime are primary concerns for the Alliance's members. For example, in the domain of Internet security and law enforcement (both key issues for the Alliance), a special body was established, known as the Law Enforcement and Security Council (LESC). This is a forum where Internet companies promote consumer confidence and trust in the Internet by coming together to address consumer security issues. Specifically, the Council wants to establish a process by which to address security on the Internet, with education as a recurring theme for both

---

[6] This paragraph is taken from: Rathmell and O'Brien, *Information Operations: An International Perspective*.

[7] See: www.internetalliance.org. See also: Rathmell and O'Brien, *Information Operations: An International Perspective*.

law enforcement agencies and consumers. Recognising problems and assessing the best course of action will be fundamental to solving these problems, the IA argues. This strategy will consist of applying and interpreting the law to address security problems on the Internet, also with an opportunity for law enforcement agencies that have previous experience in combating Internet crime to assist others who have less training.

In this context, an important White Paper was released as G8 leaders met in May 2000 for a three-day conference on 'A Government/Industry Dialogue on Safety and Confidence in Cyber-space'.

The document was delivered to government representatives who confirmed the need for self-regulation in dealing with computer and Internet crime. The report echoes earlier studies and calls for greater co-operation in battling cyber-criminals. The increase in all types of cyber-crimes is making it difficult for law enforcement agencies to keep up with the workload, creating a demand for computer security experts, the Internet Alliance says. The report states that most online crime is 'offline' crime that just happens to occur in a new medium. Therefore, the 'primary guiding principle' is how to apply laws already in the books to offences committed on the Internet. While there needs to be greater co-operation among computer security experts in the private sector, they do not want to be forced into the role of policing the Internet. 'Industry co-operation with law enforcement should be both voluntary and within the limits of the current law,' notes the report.[8] The paper also called for stronger government-industry co-operation in countering offensive Information Warfare (IW) attacks.[9]

The Alliance for Global Business (AGB)

The Alliance for Global Business (AGB) is a co-ordinating mechanism of leading international trade associations aimed at providing business leadership on information society issues and electronic commerce. Jointly, these organisations represent the bulk of electronic commerce in almost all countries in the world. The coalition represents a diverse cross-section of business in over 140 countries. Membership includes providers and users of information technology, large multinational enterprises and small start-ups, and companies in developing, as well as developed economies.

The AGB was created in response to the need for a coherent and unified global industry voice to international organisations and governments around the world. The Alliance represents a broad range of industry with a focus on high-tech manufacturers, service providers, and information technology users from nearly every sector of the global economy.[10]

The founding members of the Alliance are:

- Business and Industry Advisory Committee to the OECD (BIAC);
- Global Information Infrastructure Commission (GIIC);
- International Chamber of Commerce (ICC);

---

[8] "Seeking a Global Answer to Cyber-crime - Corporate Study Calls for Police Co-operation, Education", ABMNews.com: www.uplink.com.au/lawlibrary/Documents/Docs/Doc75.html

[9] Internet Alliance, *An International Policy Framework for Internet Law Enforcement and Security: An Internet Alliance White Paper* (May 2000): www.internetalliance.org/policy/leswp.html

[10] This section is taken from www.giic.org/agb

- International Telecommunications Users' Group (INTUG); and
- World Information Technology and Services Alliance (WITSA).

The varied membership of the Alliance for Global Business, reflecting the growing convergence between information and communication technologies, is having a profound impact on the development of international norms and rules in the areas of Information Security and CIP.

The Alliance has issued a set of fundamental principles as the basis for policymaking in electronic commerce. In 1998, the *Global Action Plan for Electronic Commerce*[11] was issued, calling for minimal government regulation and emphasising business self-regulation as the most effective way of building confidence in transactions over open networks. The initial version of the plan was officially submitted to OECD governments at the October 1998 OECD Ministerial Conference on Electronic Commerce.[12] The plan sets out the industry's views on the full range of e-commerce issues, including privacy, cryptography, consumer protection in the online environment, taxation of e-commerce, intellectual property protection, standards, competition, and Internet governance. In addition, the plan describes in detail business initiatives in all these fields, so that governments are informed of the extent to which self-regulation is already operating and what further initiatives are under development. The plan's stated aim is to create trust in ecommerce across the whole spectrum of providers for services and goods.[13]

The Alliance aims to draft a common set of definitions and best-practice guidelines for authentication and, in particular, certification practices, while, at the same time, supporting the freedom of contract to establish parties' rights and responsibilities when using electronic signatures. Similar requests and positions were confirmed in a discussion paper issued by the Alliance in April 1999 in response to a call for the World Trade Organisation (WTO) to begin an e-commerce work programme.[14] In working with the WTO, AGB has produced this discussion paper examining all trade-related issues relating to global electronic commerce, taking into account the economic, financial, and developmental needs of developing countries, with recommendations for action.[15]

Business and Industry Advisory Committee to the OECD (BIAC)

The Business and Industry Advisory Committee to the OECD (BIAC) was established in March 1962 as an independent organisation officially recognised by the OECD as being representative of business and industry. BIAC's role is to provide the OECD and its member governments with constructive comments based on the practical experience of the business community.

BIAC carries out its work through a network of policy groups that respond to and work with the different OECD Directorates and Committees. Through its consultative status *vis-à-vis* the OECD, BIAC aims to give the business community a chance to shape the development of long-term policies in OECD countries. Policy areas of the Committee range from trade liberalisation and sustainable development to e-commerce taxation and biotechnology.[16]

---

[11] www.giic.org/focus/e-commerce/agbecplan.html

[12] www.ottawaoecdconference.org

[13] www.giic.org/agb

[14] Rathmell and O'Brien, *Information Operations: An International Perspective*.

[15] The paper is available at www.giic.org/agb/agb_wtoApril1999.pdf

[16] See: www.biac.org

For several decades, BIAC has been deeply involved in the OECD's work on information, communications, and electronic commerce, through direct participation at several policy initiatives undertaken by the Committee for Information, Computer, and Communication Policy. In particular, BIAC had a major impact in overcoming many proposed government restrictions concerning cryptography during the negotiations that led to the 1997 Guidelines for Cryptography.[17]

Global Information Infrastructure Commission (GIIC)

The Global Information Infrastructure Commission (GIIC) is an independent, non-governmental initiative involving leaders from developing as well as industrialised countries. The mission of the CEO-level business organisation is to foster private sector leadership and private-public sector co-operation in the development of information networks and services to advance global economic growth, education, and quality of life.

The GIIC's goals are to strengthen the leadership role of the private sector in the development of a diverse, affordable, and accessible information infrastructure; to promote the involvement of developing countries in the building and utilisation of truly global and open information infrastructure; and to facilitate activities and identify policy options that foster effective applications of telecommunications, broadcasting, and information technologies and services.

The GIIC's three primary foci are Global Electronic Commerce, GII Development, and Education in the Information Age.

By examining policy options and promoting collaboration between governments, the private sector, and international organisations, GIIC aims to harmonise regulations and standards to support the development of the global information infrastructure.[18] At the same time, the objective is to bring developing countries into the new economy. Also relevant is that the GIIC acts as an educational and information clearing house where business representatives can pool experiences and best practices in Internet-related activities.[19]

International Telecommunication Users' Group (INTUG)

The International Telecommunications Users Group (INTUG) is an alliance of associations of telecommunications users' groups, corporations, and individuals. Established in 1974 in the Netherlands and currently based in Brussels, INTUG exists to ensure that the users' voice is heard wherever telecommunications policy is decided. As a non-profit organisation, the Group has interfaces with EC, ITU, and OECD.[20] The organisation has been very successful in interacting with national government policy-makers, both inside and outside various international fora.

INTUG concerns itself with four major issues: monopoly authority and the rights of users, free access to telecommunication networks, freedom in user choice of equipment and services, and constructive co-operation between public authorities and users.[21]

---

[17] Rathmell and O'Brien, *Information Operations: An International Perspective*.

[18] www.giic.org/agb

[19] Rathmell and O'Brien, *Information Operations: An International Perspective*.

[20] For an elaborate overview of the history of INTUG, see www.intug.net and www.intug.net/agb

[21] What is INTUG? www.hkbu.edu.hk/~hktug/newsltr/intug.html

World Information Technology and Services Alliance (WITSA)

The World Information Technology and Services Alliance (WITSA) is a consortium of 41 information technology industry associations from economies around the world. WITSA members represent over 97 percent of the world's IT market. As the global voice of the IT industry, WITSA is dedicated to advocating policies that advance the industry's growth and development; facilitating international trade and investment in IT products and services; strengthening WITSA's national industry associations through the sharing of knowledge, experience, and critical information; providing members with a vast network of contacts in nearly every geographic region of the world; and hosting events like the World Congress on IT, the Global Public Policy Conference, and the Global Information Security Summit.

Founded in 1978 and originally known as the World Computing Services Industry Association, WITSA has increasingly assumed an active advocacy role in international public policy issues affecting the creation of a robust global information infrastructure, including increasing competition through open markets and regulatory reform; protecting intellectual property; encouraging cross-industry and government co-operation to enhance information security; bridging the education and skills gap; reducing tariff and non-tariff trade barriers to IT goods and services; and safeguarding the viability and continued growth of the Internet and electronic commerce.

WITSA feels that it has a real impact on the global IT environment. The Association strengthens the industry at large by promoting a level playing field and by voicing the concerns of the international IT community in multilateral organisations, including the WTO, the OECD, the G8, and other international fora where policies affecting industry interests are developed. WITSA recently issued statements on the WTO Agreement on Basic Telecommunications Services, the Year 2000 transition, and electronic commerce.[22]

Global Business Dialogue on Electronic Commerce (GBDe)

The Global Business Dialogue on Electronic Commerce (GBDe) is a worldwide, CEO and Board-member-driven initiative to develop policies promoting global electronic commerce.

In 1998, then-EU Commissioner Martin Bangemann called on the international business community to work together with the European Commission and individual national governments in order to create an efficient and effective regulatory and legal framework for electronic commerce. The business community responded to this invitation by forming the Global Business Dialogue on Electronic Commerce, an advocacy group uniting over sixty Chief Executive Officers and other senior executives from the leading international telecommunications and IT companies.[23]

Established in January 1999, the organisation consists of major companies engaged in e-commerce worldwide and of trade organisations and is designed to be their global voice on e-commerce issues. The objective is to address political decision-makers around the world in a unified fashion, suggesting ways to avoid conflicting policies and patchwork legislation. Where regulation cannot be avoided, the GBDe proposes to work with governments and international organisations to develop business-led, self-regulatory systems that create consumer confidence and maintain efficiency.

---

[22] www.witsa.org

[23] Rathmell and O'Brien, *Information Operations: An International Perspective*.

At its inception, the GBDe established a number of issue groups tackling many issues related to e-commerce. GBDe currently has nine of these groups: authentication and security, consumer confidence, content/commercial communications, information infrastructure (including interoperability and internet governance), intellectual property rights, jurisdiction, liability, protection of personal data, and tax and tariffs.[24]

The objective of these working groups was to foster debate amongst members and to produce detailed policy recommendations for governments and other international organisations such as the Geneva-based World Trade Organisation. In September 1999, the working groups presented the initial findings of their activities at the first annual GBDe conference held in Paris. Information security was one of the urgent topics discussed by the many CEOs and senior officials attending the two-day event. Their initial conclusions called for strong co-operation between governments and international businesses in countering the increasing number of malicious activities over the Internet. They believed that it was vital that the security of electronic transactions be protected in order to ensure the trust of both business and consumers in electronic commerce. Therefore, 'governments, administrations, parliaments and international organisations should provide a minimal legal framework to ensure the legal effectiveness of electronic authentication methods and should preferably rely on existing law to deter fraud and other misconduct." [25] In order to achieve these objectives, the working groups called for the full legal recognition of electronic signatures and the removal of legal restrictions on the use and export of encryption.

During 2000, the GBDe contributed to the G8 summit meeting on information technology. In an Information Technology Charter, a new standard was set for e-commerce policies globally, regionally, and nationally. During this period of time, the GBDe also worked with a number of international organisations including the OECD, the WTO, the United Nations Development Program (UNDEP), and the World Bank (WB), providing input and adding the practical business perspective to broad policy deliberations. In addition, the GBDe has signed co-operation agreements with key business organisations such as the ICC (see above), BIAC (see above), the eASEAN Task Force, and the APEC Business Advisory Council.[26]

In September 2000, the working groups released a document detailing a set of policies and action-plans against cyber-crime and other offensive Information Warfare activities. The overall objective of these efforts is to "begin co-operative, international industry-to-government and government-to-government efforts to enhance cyber-security and to fight cyber-crime".[27] The GBDe has invited companies and governments to increase their investments in Information Assurance and cyber-security products, services, and procedures to protect "the value of their business, and government information and content". Particular attention has been devoted to issues relating to state-sponsored industrial espionage and information sharing. Concerning the former, this industry body has condemned "any state-sponsored industrial espionage to advance the commercial interest of companies or nations", and calls for its members "to pledge not to accept competitive information from such sources". The GBDE strongly supports the creation of information-sharing schemes concerning information security.[28]

According to the GBDe, businesses responsible for network infrastructure have a responsibility to work together to promote information security in co-operation with governments. In addition to

---

[24] See also the GBDe brochure at: www.gbd.org/acrobat/brochuresm.pdf. More on the origins of GBDe can be found on their website at: www.gbd.org

[25] Information taken from the GBDe's website at www.gbde.org

[26] See the GBDe brochure at: www.gbd.org/acrobat/brochuresm.pdf

[27] GBDe, "Cyber-Security and Cyber-crime" – Statement issued on 15 September 2000

[28] This paragraph is taken from Rathmell and O'Brien, *Information Operations: An International Perspective*.

co-operation on sharing information with other enterprises and government about potential threats, attacks, viruses and cyber-crime incidents, businesses should work together to reduce vulnerabilities and improve protective measures. To promote such co-operation, the GBDe has urged business in all regions to establish voluntary information sharing mechanisms regarding cyber-attacks, vulnerabilities, countermeasures, and effective information security practices.[29]

With the belief that the future of the digital economy hinges on a secure Internet, and that there exists a rapidly increasing need to improve cyber-security and fight cyber-crime, the GBDe formed a special Working Group. The Cyber-Security Working Group was officially launched on April 26, 2000 in New York City, at a meeting of the GBDe Business Steering Committee.[30]

During the GBDe 2000 Miami Conference in September that year, the GBDe Cyber-Security paper was presented, including an extensive and detailed list of policy recommendations for both industry and government action.[31] The GBDe is providing these recommendations to all governments, at all levels, so as to begin co-operative, international industry-to-government and government-to-government efforts to enhance cyber-security and to fight cyber-crime.

Consumers International (CI)

Consumers International (CI) supports, links and represents consumer groups and agencies all over the world. It has a membership of more than 260 organisations in 119 countries. Most members are independent, non-governmental organisations.

IC strives to promote a fairer society through defending the rights of all consumers, including poor, marginalised and disadvantaged people, by supporting and strengthening member organisations and the consumer movement in general; and by campaigning at the international level for policies which respect consumer concerns.

Consumers International is an independent, non-profit organisation. It is not aligned with or supported by any political party or industry. It is funded by fees from member organisations and by grants from foundations, governments and multilateral agencies.

The organisation was founded in 1960 as the International Organisation of Consumer Unions (IOCU) by a group of national consumer organisations that recognised that they could build upon their individual strengths by working across national borders. The organisation rapidly grew and soon became recognised as the voice of the international consumer movement on issues such as product and food standards, health and patients' rights, the environment and sustainable consumption, and the regulation of international trade and of public utilities.

Consumers International's Head Office is based in London, as is its Office for Developed and Transition Economies. Regional Offices are located in Kuala Lumpur (Malaysia), Santiago (Chile) and Harare (Zimbabwe).[32]

Besides activities and achievements such as consumer protection, consumer education, institution and capacity building, and the provision of a variety of publications, e-commerce is one of the focus areas. Consumers International claims to have been at the forefront in consumer activism in the new area of ecommerce and has contributed extensively to the development of OECD

---

[29] Brochure GBDe at: www.gbd.org/acrobat/brochuresm.pdf

[30] See www.gbde.org/cyber-security/

[31] Available at: www.gbde.org/cyber-security/cs2000.html

[32] Taken from: www.consumersinternational.org

guidelines for consumer protection in e-commerce. CI has also carried out research on consumer satisfaction with regard to Internet shopping, as well as working on other important issues such as privacy and alternative dispute resolution in Internet transactions.[33]

Publications during 2001 related to e-commerce include advice and guidance for shopping on the Internet[34] and the results of a comparative study of privacy protection on 751 Internet sites for consumers. The main findings of this study revealed that existing measures put in place by various governments to protect people's privacy inadequate: many European and American Internet sites aimed at consumers fall woefully short of international standards on data protection.[35]

Earlier studies were, amongst others, 'Disputes in Cyber-space - on-line dispute resolution for consumers in cross-border disputes'[36] and several studies on consumers' online shopping.[37]

As can also be concluded from last year's annual report, CI has contributed to new international guidelines and conducted research on Internet shopping, mechanisms for dispute resolution, and privacy:[38]

- Concerns about surveillance and unauthorised use of personal information collected over the Internet by business were discussed in a workshop in the Netherlands for CI members from Europe, Latin America, and Asia.

- A new CI study of privacy protection on more than 750 Internet sites, Privacy@net, was prepared for release in early 2001.

- CI continued to work with the OECD Consumer Policy Committee on the implementation of its Guidelines for Consumer Protection in Electronic Commerce. 'Disputes in Cyber-space', a new CI study released at an OECD meeting in December2001 found that no on-line dispute resolution service meets all criteria for good practice. The survey assessed providers of on-line business to consumer dispute resolution services using recommendations from the Transatlantic Consumer Dialogue and the European Commission. This report, as the first of its kind, generated considerable media interest.

- Consumer groups in the UK, Holland, Argentina, and elsewhere are encouraging best practice in the form of Web Trader seals for e-businesses.

- Dozens of CI members around the world participated in the US Federal Trade Commission's Millennium Surf to fight fraud on the Internet. The sweep targeted get-rich-quick schemes promoted over the Internet with consumer groups from the UK to Uruguay sending information to the FTC on some 1,600 suspect web sites.

---

[33] See www.consumersinternational.org/campaigns/index.html#electronic

[34] www.consumersinternational.org/CI_Should_I_buy.pdf

[35] Full report available at: www.consumersinternational.org/news/pressreleases/fprivreport.pdf

[36] www.consumersinternational.org/campaigns/electronic/adr_web.pdf

[37] See: www.consumersinternational.org/campaigns/index.html#electronic

[38] See Consumers International *Annual report 2000*: available at www.consumersinternational.org/annualreport/2000/AR30-35.pdf

References

Rathmell, Andrew, and Kevin A O'Brien. *Information Operations: An International Perspective* – Special Report. Jane's Information Group: December 2000.

Internet Alliance. *An International Policy Framework for Internet Law Enforcement and Security: An Internet Alliance White Paper*. (May 2000): www.internetalliance.org/policy/leswp.html

'Seeking a Global Answer to Cyber-crime – Corporate Study Calls for Police Co-operation, Education"' www.uplink.com.au/lawlibrary/Documents/Docs/Doc75.html

GIIC. 'Drive to boost consumer confidence in e-business'. Press release (11 October 1999): www.giic.org/pr991011.html

GBDe, *The GBDe Cyber Security paper presented at the GBDe 2000 Miami Conference 2000*: www.gbde.org/cyber-security/cs2000.html

Consumers International, *Annual Report 2000*: www.consumersinternational.org/annualreport/2000/AR30-35.pdf

ICC, 'Cyber-crime bulletin urges victims to share information'. Press release (12 January 2000): www.iccwbo.org

Other Sources

Information Assurance Advisory Council www.iaac.org.uk

International Chamber of Commerce (ICC) www.iccwbo.org

ICC Cyber-crime Unit www.iccwbo.org/ccs/menu_cyber-crime_unit.asp

The Internet Alliance website www.internetalliance.org

Alliance for Global Business (AGB) www.giic.org/agb

Business and Industry Advisory Committee to the OECD (BIAC) www.biac.org

International Telecommunication Users Group www.intug.net

World Information Technology and Services Alliance www.witsa.org

Global Information Infrastructure Commission www.giic.org/agb

GBDe www.gbde.org

Consumers International www.consumersinternational.org

COUNCIL OF EUROPE (COE)

Socio-Political, Economic, and Commercial Overview

The Council of Europe (COE), headquartered in Strasbourg, France, is continental Europe's oldest political organisation, founded in 1949, and consisting of 43 countries[1] and having granted observer status to five more.[2] The COE is distinct from the 15-nation European Union, however: no country has ever joined the EU without first becoming a member of the Council of Europe. The Council was devised to develop agreements to standardise member-countries' social and legal practices in a manner that defends human rights, democracy, and criminal justice.

The COE consists of :

- Committee of Ministers: the COE's decision-making body, composed of the 43 foreign ministers or their Strasbourg-based deputies (ambassadors / permanent representatives).
- Parliamentary Assembly: 602 members (301 representatives and 301 substitutes) from the 43 national parliaments and Special Guest delegations from the two parliaments of east European non-member states. The current President is Lord Russell-Johnston of the UK.
- Congress of Local and Regional Authorities
- Secretariat of Secretary-General Walter Schwimmer (Austria). [3]

The COE's main legal instruments are conventions and recommendations. Recommendations are directed towards member-states and provide guidelines for national legislation or administrative practices. Conventions are binding to ratifying states, while recommendations are not. Pertinent to issues of ICT dependability, the COE monitors 'potential technological and scientific developments in order to prepare related regulations and principles.'[4]

The COE plays a leading role, at the European as well as the global level, in monitoring legal issues related to human and social rights and criminal justice. In particular, COE tries to shape common European legislation by fostering harmonisation of national legislations and monitoring potential technological and scientific developments in order to prepare related regulations and principles. The COE directs recommendations to member-states and provides guidelines for national legislation or administrative practices. The COE's activities usually conclude in either conventions or recommendations. The former are considered to be the essential element of the COE's supporting activities for legal co-operation, as they are binding to those states that sign and ratify them. Unlike conventions, recommendations are not binding.

The COE's involvement in issues relating to cyber-crime began at the end of the 1980s. In 1990, the Council's Committee on Crime Problems released a recommendation highlighting various

---

[1] Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, the Netherlands, Norway, Poland, Portugal, Romania, Russia, San Marino, Slovakia, Slovenia, Spain, Sweden, Switzerland, "The former Yugoslav Republic of Macedonia", Turkey, Ukraine, and the United Kingdom.

[2] The Vatican, the United States, Canada, Japan, and Mexico.

[3] Council of Europe Portal: press.coe.int/files/e-cebref.htm

[4] Rathmell and O'Brien, "Council of Europe", *Information Operations – An International Perspective*.

aspects of the fight against computer crime.[5] This document identified many areas requiring immediate attention from scholars and practitioners of criminal law. First, there were questions concerning computer-related fraud, such as the entering, erasing, or modifying of computer data with fraudulent intent. A second problem was computer forgery, which is the illegal input, alteration, erasure, or suppression of computer data and computer programs. Likewise, the Committee highlighted cases of the unauthorised change or modification of data and computer programmes, as well as the possibility of carrying out so-called 'computer sabotage'. The recommendation referred also to unauthorised access or interception of computer and network systems, as well as the illegal reproduction of hardware and software solutions. The importance of this recommendation relates to the fact that it was one of the first major international efforts towards the harmonisation of computer crime legislation. Nevertheless, as indicated by the document itself, there remained unresolved issues of criminal procedures in this domain, the topic of a second important COE initiative.

Analysis of the Main Regulatory and Legal Developments Related to Information and Telecommunications Systems and Services

Economic and industrial environment affecting state control of key industries: In light of the *Convention on Cyber-Crime* (see below), the COE does put considerable pressure on ISPs. However, there is nothing within the Convention which situates ISPs with an economic or industrial environment. The COE does state that the Internet has upwards of 158 million users in the world, 95 million of which are in Europe. Additionally, over 60 million computers were sold worldwide in 2000 at an annual growth-rate of 15 percent. Online sales accounted were worth US$650 billion (€747.1 billion) in 2000, and COE states that this number is projected to triple in two years. While this climate is poised to stimulate e-commerce, the COE also stresses that it 'provides a fertile medium for cyber-crime.'[6]

General legal principles and developments related to the ICT environment; overview of relevant new legislation: Most notably, issues of surveillance and copyright infringement have been overhauled with respect to the Internet. See below for the descriptions of the Cyber-crime Convention and Recommendation Nos. R(2001)8 and R (99)5.

Regulatory initiatives to guide the provision of new information and network services: Article 35 of the *Convention on Cyber-Crime* calls for the creation of a '24/7 Network' where 'each Party shall designate a point of contact available on a 24 hour, 7 day per week basis in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of criminal offence.'[7]

Assessment of Phenomena Undermining Dependability

As a beneficial result of the lengthy process of the construction of the Cyber-crime Convention, the COE has deliberated on the spectrum of crimes enabled or exacerbated by ICT. These crimes are seen not only to hinder development opportunities and e-commerce but also have detrimental effects on the rights of citizens.[7]

---

[5] Council of Europe, Computer Related Crime: Recommendation R(89)9 on Computer Related Crime and Final Report of the European Committee on Crime Problems (Strasbourg, 1990).

[6] COE Portal: press.coe.int/dossiers/107/E/e-village.htm

[7] *Council of Europe Convention on Cyber-Crime.* Title 3, Article 35, Paragraph 1

COE gives a few outstanding examples of crimes undermining dependability of ICT:[8]

Child pornography: 350,000 to 500,000 pornographic photographs of children are freely available on the Internet. In the space of a year, the number of German-language child-pornography sites doubled - and one of them attracted 500,000 surfers. US Customs recently dismantled a Moscow-based network trading in pornographic videos featuring underage children. The COE feels that while governments may be trying to improve their laws to deal with the problem, the only effective response is international co-operation. *Note: a few documents by the COE wrongly use 'paedophilia' and 'child pornography' interchangeably; paedophilia is an abstract state of mind while child pornography is an action undertaken by some paedophiles.*

Racism: Anti-racist associations report that racist sites are proliferating on the Internet. Roughly 160 sites of this kind were operating from the US in 1995 and the number has grown now to over 2,500. The COE cites 'some experts' as putting the number of sites openly encouraging racial violence at about 4,000 These sites disseminate hate-filled propaganda and revisionist texts, 'black lists', and neo-Nazi cult items such as swastikas, CDs, videos, etc. The free-speech guarantee written into the First Amendment to the US Constitution makes this issue especially problematic. *Note: the COE Portal (wrongly) uses the term 'skinhead' synonymously with 'racist).*

Viruses, Worms, and Trojan horses: There is a demonstrated vulnerability to viruses. For example, the financial damage inflicted by the 'I Love You' virus is estimated to be in the billions. This virus infected 65 percent of American firms with over 200 employees and succeeded in causing the Swiss Government's email system to shut down for more than 24 hours. (COE Portal). The COE cites the FBI figure for the production of viruses, worms, and other Trojan horses at an average of 50 per week. Additionally, there are 'a good hundred' do-it-yourself virus kits available. The COE speculates of 'good times ahead' for the anti-virus industry.

'Pirates' and Mafiosi: The COE gives the example of an incident where four 'hackers' broke into the confidential file on the 1,400 participants at the recent 2000 World Economic Forum (WEF) in Davos, Switzerland, and obtained information such as credit card numbers and expiry dates, private addresses, and mobile phone numbers of many world leaders and other notables. Recently, organised gangs of cyber-criminals in Russia and the Ukraine mined over 40 US sites and succeeded in obtaining at least one million credit card numbers. *Note: problematic use of the term 'hacker.'*

Regarding all phenomena undermining dependability, the COE delineates four areas of criminal activity within its Cyber-crime Convention:[9]

1. Offences against the confidentiality, integrity, and availability of computer data and systems. This includes illegal access, illegal interception, data interference, system interference, and illegal device;

2. Computer-related offences such as computer-related forgery and fraud;

3. Content-related offences such as child pornography and racism; and

4. Offences related to infringements of copyright and related rights.

---

[8] All examples found on COE Portal: www.coe.int/T/E/Communication_and_Research/Press/Themes_Files/Cyber-crime/e_crimes.asp#TopOfPage

[9] *Council of Europe Convention on Cyber-Crime*: conventions.coe.int/Treaty/EN/projets/FinalCyber-crime.htm

Organisational Initiatives Aimed at Tackling Cyber-Security/Cyber-Crime or Assisting with the Development of Dependability

The COE feels that many countries' laws are not up to the challenges posed by cyber-crime. The Council cites a survey done by the US firm McConnell International that found only ten countries that had 'significantly' altered their laws to deal with unique aspects of cyber-crime, with around ten counties having partially updated them, while thirteen others were preparing to do so. At a Council of Europe Parliamentary Assembly's hearing in March 2001, an American expert was cited for making two 'important points': 'laws are needed to make cyber-space safe, and countries with inadequate laws will be less competitive on the new economic markets.'[10]

The Council of Europe's first recommendation on cyber-crime was agreed upon in 1989,[11] followed by a second one in 1995 on aspects of criminal procedural law. This second recommendation put forward the idea of an international treaty on cyber-crime.[12] Recommendation R(95)13 recognised the need for a common international criminal law approach to issues related to information and network technologies and outlined recommendations concerning criminal procedural law in the realm of information and network technologies.[13] R(95)13 stressed that criminal procedure laws of member-states rarely provide powers to search and seize, regardless of the fact that it is possible for evidence of criminal offences to be stored and transferred by information and network systems. There was, therefore, the need for a common international criminal law approach to issues related to information and network technologies. The Recommendation covered problems of and possible solutions for search and seizure; technical surveillance; electronic evidence; the potential obligation of natural and legal persons to co-operate with law enforcement; the need for research activities and statistics for the monitoring of technological and criminal developments; advanced training for lawmakers, lawyers, and police personnel; and the review of national legislation and strong international co-operation.[14] In order to achieve these objectives, the document proposed that states should review their national legislation and practices. In addition, states should ensure that investigating authorities and other professional bodies were aware of the contents of the recommendations.

In February 1997, the Council of Europe's Committee of Ministers instructed a new committee (the Committee of Experts on Crime in Cyber-space) to prepare a binding legal instrument, and to consider questions relating to cyber-crimes, substantive criminal law, the use of coercive powers, and jurisdiction in cases of cyber-crime. In June 1997, the European Ministers of Justice issued a resolution supporting the activities of the European Committee on Crime and the Committee of Experts on Crime in Cyber-space. Between April 1997 and December 2000, the Committee of Ministers held ten plenary meetings, and its drafting group fifteen meetings, to work towards definitions of common legal and regulatory responses to the risks posed by emerging information technologies. After the more than two years of debates and meetings, a draft *Convention on Cyber-Crime* was assembled. In April 2000, the draft text was declassified and published on the Internet in order to undergo the scrutiny of specialists and network users. The Draft *Convention on Cyber-Crime* was formally released in May 2000.[15]

---

[10] COE Portal: www.coe.int/T/E/Communication_and_Research/Press/Themes_Files/Cyber-crime/e_crimes.asp#TopOfPage

[11] Council of Europe, Recommendation No. R(89)9. (Strasbourg, 1995).

[12] Council of Europe, Problems of Criminal Procedural Law Connected with Information Technology Recommendation R(95)13 and Explanatory Memorandum (Strasbourg, 1995).

[13] Council of Europe, Recommendation R(95)13 (Strasbourg, 1995).

[14] Rathmell and O'Brien, "International Organisations and Developments", *Information Operations – An International Perspective*.

[15] Rathmell and O'Brien, "International Organisations and Developments", *Information Operations – An International Perspective*.

In March 2001, international experts on ICT were invited to comment on the draft during a special session of the Parliamentary Assembly. The Assembly issued recommendations regarding the draft to the Committee of Ministers, which were adopted with amendments at the April 2001 session. Committee of Ministers' deputies approved the Convention's text on 19 September 2001 and the Foreign Ministers formally adopted the Convention on 8 November 2001. The *Convention on Cyber-Crime* was ratified by signature of the member-states on 23 November 2001 in Budapest.

Also of Note:

- Recommendation No. R(2001)8 concerning self-regulation is covered below, sub-section (iii).

- Recommendation No. R(99)5 covers guidelines to both users of the Internet and ISPs. See below, sub-section (iii).

Central policy and operational co-ordination mechanisms: The Convention comes into force once five nations, three of which must be COE members, sign the document.

Article 1 of the Convention covers definitions particular to the Internet and communication technologies. Afterwards, Chapter II covers measures to be undertaken at the national level. Articles 2-13 define and outline classes of offences to be considered in the substantive criminal law (see Section 3, p. 5): offences against the confidentiality, integrity and availability of computer data and systems (such as illegal access, interception, and data and system interference and misuse of devices); computer-related offences (such as forgery and fraud); content-related offences (child pornography); and offences related to infringements of copyright and related rights (such as copyright violation). Issues of procedural law, such as the scope of laws, safeguards, collection and preservation of computer data, and traffic information, search and seizure, as well as issues of jurisdiction of the member-states and international co-operation regarding procedural law - such as extradition and mutual assistance - are also covered. Specific problems of preservation of data – including traffic data - stored in a computer system are also addressed.

Chapter III covers international co-operation regarding cyber-crimes. Article 24 through 35 delineate provisions regarding extradition, mutual assistance, the giving of spontaneous information, confidentiality and limitations on use, the preservation of stored data, disclosure and mutual assistance regarding preserved and real-time traffic data, and the 24/7 network (see below).

Government institutions dealing with cyber-crime: The *Convention on Cyber-Crime* makes procedural requests of the member-states, but issues no recommendations or requests towards specific government institutions. Due to the EU's principle of subsidiarity, it is unlikely that the COE would ever advocate an overarching inter-governmental institution to deal with cyber-crime. However, Article 35 of the *Convention* calls for the creation of a '24/7 Network' where 'each Party shall designate a point of contact available on a 24 hour, 7 day per week basis in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of criminal offence.'[16]

Government-sponsored schemes aimed at enhancing the security of information and network systems: Apart from what is already stated regarding the Convention in sub-section (i), there are two recommendations dealing with the security of information:

---

[16] This may be a measure that the COE has taken in response to the G8-sponsored initiative to establish national contact-points to facilitate co-operation. Rathmell and O'Brien, "International Organisations and Developments", *Information Operations – An International Perspective*. See *Council of Europe Convention on Cyber-Crime*, Title 3, Article 35, Paragraph 1: conventions.coe.int/Treaty/EN/projets/FinalCyber-crime.htm

Recommendation No. R(2001)8 outlines recommendations concerning 'self-regulation and user protection against illegal or harmful content on new communications and information services.' Topics included in the recommendation are: self-regulatory organisations, content descriptors, content selection tools, content complaint systems, mediation and arbitration of disputes, content-related matters, and user information and awareness.[17]

Recommendation No. R(99)5 covers guidelines for both Internet users and ISPs. This document delineates the responsibilities of users and ISPs and states that the 'Users should be aware of the responsibilities of ISPs and vice versa'. Towards users, the recommendations stressed that the Internet is not secure and outlines basic security precautions and responsibilities. Notably, the recommendation states that 'anonymous access to and use of services, and anonymous means of making payments, are the best protection of privacy'; however, 'complete anonymity may not be appropriate because of legal constraints.' Towards ISPs, the recommendation states that subscribers should be informed of 'the possibilities of accessing the Internet anonymously, and using its services and paying for them in an anonymous way' while again stating that anonymity is subject to legal constraints. ISPs are also given warnings regarding the collection, storage, and processing of data, and interference with the contents of communications.[18]

Government schemes to assess the threat or to provide warnings and response capabilities to government or private sector clients: Amendments to the *Convention on Cyber-Crime* can be made to allow for new developments (Article 44). Also relevant is Article 35 of the *Convention on Cyber-Crime* which calls for the creation of a '24/7 Network' (as discussed above).

Article 46 also declares that member-states 'shall, as appropriate, consult periodically with? view to facilitating … the exchange of information on significant legal, policy, or technological developments pertaining to cyber-crime and the collection of evidence in electronic form…' and to consider 'possible supplementation or amendment of the Convention.' In particular, the European Committee on Crime Problems is charged with facilitating these consultations and 'conduct a review of all the Convention's provisions and, if necessary, recommend any appropriate amendments.'[19]

Public-Private Partnerships

As part of its consultations on the Convention on Cyber-crime, the COE convened a Panel of Experts drawn from outside the Council. This working group on cyber-crime is chaired by Prof. Kaspersen of the University of Amsterdam. A number of non-members are also represented as observers to the ad-hoc group – including the US, Canada, Japan, South Africa, the European Commission, the OECD, UNESCO, and others. The Committee of Experts was responsible for the Convention on Cyber-crime.[20]

---

[17] Council of Europe Recommendation (2001)8: *Recommendation Of The Committee Of Ministers To Member States On Self-Regulation Concerning Cyber Content.*

[18] Council of Europe Recommendation R(99)5: *Recommendation Of The Committee Of Ministers To Member States For The Protection Of Privacy On The Internet; Guidelines For The Protection Of Individuals With Regard To The Collection And Processing Of Personal Data On Information Highways*. Adopted by the Council of Europe Committee of Ministers on 23 February 1999 at the 660th meeting of the Ministers' Deputies.

[19] *Council of Europe Convention on Cyber-Crime*, Article 46: conventions.coe.int/Treaty/EN/projets/FinalCyber-crime.htm

[20] Privacy International, *Cyber-Crime: Council of Europe*: www.privacyinternational.org/issues/cybercrime/ (downloaded 28 January 2002).

GROUP OF EIGHT (G8)

The G8 (UK, USA, France, Germany, Japan, Canada, Italy, and Russia, with the European Union having observer status) has been meeting since 1975 and since 1995 has become more and more involved in issues relating to cyber-crime, although discussions have also taken place in the past relating to information society, terrorism, and crime generally. Information society emerged as an official topic with the publication of the Okinawa Charter on Information Society, published in 2000. Other work has mostly been concerned with cyber-criminality and with international responses to cyber–crime and cyber–terrorism.

Socio-Political, Economic, and Commercial Overview

The issues of cyber-crime and cyber-terrorism – and, along with those, issues of dependability and information assurance – have seen a steady rise up the G8's agenda. A special working group of Senior Experts on Organised Crime, called the 'Lyon Group' was set up in 1995 at a summit meeting in Halifax, Canada. The Group released a series of recommendations to combat transnational organised crime efficiently (informally called 'The 40 Recommendations') on 12 April 1996 Foreign Ministers and Ministers responsible for security then met in 1996 to discuss terrorism. During this meeting, Ministers of member-nations called upon states to note the increasing use of 'electronic or wire communications systems and networks'. They emphasized the need to find means, consistent with national law, to stop such activity.

January 1997 saw the chair of the G8 pass to the United States and the creation of a 'Sub-Committee on High-Tech Crime', chaired by a representative from the Department of Justice. At the Denver summit in June 1997, this issue was raised to Head of State level and a *communiqué* was issued, mentioning the need to intensify efforts to implement the Lyon recommendations. A separate Foreign Ministers' report was published with a number of further recommendations concerning the tracking of users.

In October 1997, the 'Carnegie Group' (Expert Group to G8 ministers and Chief Advisors of Science and Technology) released what many saw as a contradictory report on 'Misuse of International Data Networks'. At the May 1998 Birmingham summit in the United Kingdom, a further *communiqué* was issued which endorsed principles released in December 1997. A Virtual Meeting on Organised Crime and Terrorist Funding was held in December 1998, at which G8 Justice Ministers participated via videolink. This meeting re-emphasized the importance of the 24-hour law enforcement response network.

Cyber-crime was next mentioned at the Moscow meeting on Combating Transnational Organised Crime in October 1999, where G8 Justice Ministers released another *communiqué* that included principles on access to files, and also had an extensive annex discussing the issue of stored data. May 2000 saw a meeting take place in Paris to develop recommendations on cyber-crime for presentation to the 2000 Okinawa summit in Japan. The final Paris *communiqué* identified the need for public-private partnerships to assist in the development of novel solutions for 'crime that has an electronic component'.

Seizing Digital Opportunities: Importance of building on key foundations: economic and structural reforms to foster open, efficient use of the new technologies; sound macroeconomic management for exploitation of new information technologies, the development of information networks offering fast, reliable, secure, and affordable access through competitive market conditions and related innovation; development of human resources for the information age; and finally, active utilisation of IT by the public sector. Apportioning of government and private sector responsibility should be of the following makeup: that the government creates a predictable, transparent, and

non-discriminatory policy that supports the role of the private sector in the development of information and communication networks.

Bridging the Digital Divide: Affirms the right of everyone to enjoy the benefits that information and communication networks provide. Commitment to the efforts underway to formulate and implement a strategy to address this issue. Key component is the drive toward universal and affordable access. These policies must also be underpinned by development of human resources commensurate with the challenges and opportunities of the Information Age.

Promoting Global Participation: Tremendous opportunity that IT presents for emerging and developing countries. Ability to 'leapfrog' conventional obstacles of infrastructural development. However, also great challenges, as some nations may miss(due to their lack of basic economic and social infrastructures) electricity and telecommunications. Necessity of an approach for each situation: diverse conditions and needs of developing countries need to be taken into account.

The Way Forward: Efforts at bilateral and multilateral co-operation at all levels and the work done by multilateral development banks in contributing to programmes that foster growth, benefit the poor, and expand connectivity, access, and training were applauded in the Okinawa Charter. Identified priorities for further concrete steps by the Digital Opportunity Task Force (DOTF), established in the Okinawa Charter (see below) and to include:

Fostering policy, regulatory, and network readiness This step concentrates upon the creation of policy advice to promote a pro-competitive and flexible policy and regulatory environment, the sharing of experience between developing countries and others, and encouragement of the use of IT in assistance of other development efforts, such as education and the reduction of poverty.

Improving connectivity, increasing access, and lowering cost is concerned with the improvement of information and communications infrastructure through the development of partnerships between governments, international organisations, the private sector, and NGOs. Community access programs are also supported, as are programs to reduce the costs of acquiring connectivity in developing countries. Other issues under this include improvement of network interoperability, services and applications, research and development adapted to the specific requirements of developing countries, and improvement of locally-relevant content in mother-tongues.

Building human capacity covers the use of ICT in education, including the use of distance learning and community-based training. This priority point also covers getting public institutions and communities networked. This also includes the provision of basic education, creation of a pool of trained IT professionals, and particular emphasis on the development of IT skills.

Encouraging participation in global e-commerce networks covers increasing e-commerce readiness and use via the provision of advice to start up businesses in developing countries and ensuring that the new emerging regulatory environment is consistent with development efforts.[1]

Analysis of the Main Regulatory and Legal Developments Related to Information and Telecommunication Systems and Services

The G8 stance on the regulatory and legal approach to information and communication systems and services is that broadly speaking, competition should be promoted in open markets as much as possible; customs duties should continue not to be levied as per the WTO moratorium on cross-

[1] www.dotforce.org/reports/it1.html

border Internet transactions; and further liberalisation and improvement in networks and telecommunications, transportation, and package delivery.

The WTO framework for the promotion of cross-border trade in electronic goods and services is also backed by the G8, as is the principles of non-discriminatory and cost-oriented telecommunication interconnection. This is also relevant to the debate on approaches to taxation of Internet commerce.

Protection of Intellectual Property Rights (IPR) is also recognised as being vital to the promotion of IT-related innovation. Finally, the G8 also accepts that the promotion of consumer trust and the creation of privacy protections according to the OECD Guidelines are areas where effective self-regulatory mechanisms can be set up.

Organisational Initiatives Aimed at Tackling Cyber-Security/Cyber-Crime or Assisting with the Development of Dependability

A strong theme throughout the history of the G8 since 1975 has been the development of its responses to the threats posed by cyber-crime and cyber-terrorism. At the Halifax summit in 1995, the Lyon Group was established and began looking at all forms of transnational criminal activities. A subgroup investigating computer crime and the illegal use of advanced technologies (known as the Working Group on High-Tech Crime) began operations from in 1997.

The ten-point principles and ten-point plan, first agreed in Washington, DC, in December 1997 by Interior and Justice Ministers, included the following:

- A review of legal systems to ensure that abuse of telecommunications and computer systems is criminalised, and that high-tech crime investigations are promoted;

- Include high-tech crime in any discussions concerning mutual assistance arrangements;

- Monitor and develop solutions (including technological ones in conjunction with the private sector) to the issues of the preservation of evidence and trans-border searches; and

- Quickly develop procedures for obtaining traffic data from communications carriers and investigate the international transfer of such data.

In April 1998, the Forty-Point 'Recommendations to combat Transnational Organised Crime' were published at the summit in Lyon, France. This reiterated the statement concerning the criminalisation of abuses of the telecommunications network and also argued for greater liaison and sharing of experience between international law-enforcement representatives and the promotion of study into this new form of crime. Interestingly, here, the relevance of electronic surveillance and undercover operations was emphasised in the ongoing struggle against cyber-crime and cyber-terrorism, although with due regard given to human rights.

The first statements regarding cyber-crime appeared in 1996, following a meeting in Paris of Foreign and Interior Ministers. States were told to make themselves aware of the new threats of '…terrorists using electronic or wire communications systems and networks to carry out such criminal acts'. To combat this, states agreed to speed up consultations on the use of encryption and the need for lawful access to data and communications to prevent or investigate acts of terrorism,

while protecting personal privacy (a debate that has still not been concluded, and may never be).[2] A further initiative that was promoted was the increased exchange of operational information by law enforcement.

January 1997 saw the creation of a Subcommittee on High-tech Crime, an initiative backed by the US government, then chairing the G7 (Russia was not yet a member). The high-tech crime subcommittee was chaired by Scott Charney, of the US Department of Justice. One of the main achievements was the creation of a 24-hour contact group for law enforcement, which would assist in communications between national law enforcement communities. At the Denver summit in June of that year, this issue was raised up to the level of national leadership. The subsequent *communiqué* stated that efforts to implement the Lyon recommendations would be intensified, and also that the investigation, prosecution, and punishment of high-tech crimes across national borders would be an area of concern in the next year, as would the provision of a legal and technical system to respond to high-tech crime.

The separate Foreign Minister's Progress Report examining these issues recommended greater identification and tracking of users, as well as the implementation of restrictions on encryption. The need for co-operation with each other in enhancing the capability of member-nations to identify, locate, and prosecute criminals, assistance in the collection of evidence, and the continuation of training in this area were all stated in the report.

The document backed the adoption of the OECD guidelines on cryptography and asked states to develop national policies on encryption that would allow government access to investigate and prevent terrorism in a manner consistent with these guidelines.

In October 1997, another group of experts, the Carnegie Group (officially the Expert Group to the G8 Ministers and Chief Advisors of Science and Technology) released a report on 'Misuse of International Data Networks'. The report was broadly criticised for recommending often contradictory legal and technical measures. US chairmanship of the G8 also saw a number of statements by the US Attorney-General Janet Reno relating to the balance between fighting these new forms of crime and protecting personal privacy.

Principles established by these comments in December 1997 were echoed in a *communiqué* issued in May 1998, under the chairmanship of the United Kingdom. The statement called for closer co-operation with industry on working towards an effective legal framework for obtaining, presenting, and preserving electronic data as evidence. The existence of the 24-hour information sharing group was publicised at the G8 virtual meeting on organised crime and terrorist funding in December of that year, where Justice ministers were able to emphasize the talks that the Lyon Group had been having with ISPs and other industry bodies on the prevention of criminal use of networks and ensuring 'traceability' of communications. A legal framework was also underway for the speedy retrieval of electronic information.

Cyber-crime was not mentioned at the next summit meeting in Cologne, but it was back on the agenda at a ministerial conference on 'Combating Transnational Organised Crime' in Moscow in October 1999. Justice Ministers present at this conference released another *communiqué* that had an extended annex on access to stored data, and included principles of access to files and identification of users. The annex also included a declaration that states should maintain a capability to secure rapid preservation of data stored in a computer system (even if necessary only to assist another state). Agreement was also reached on a proposition put forward by the Working Group on High-Tech Crime that law enforcement authorities could search computers located in

---

[2] For a discussion of recent legislation in this field, please see "Privacy and the Counter-Terrorism War", *Jane's Intelligence Review* (January 2002).

another country. However, the UK and Germany dissented on proposals concerning encryption – the UK preferred the subject to come under a separate section, whereas Germany wanted the issue of encryption to be included in the main body of the document (and thus more fully integrated into proposals). In the end, it was decided that encryption would be discussed again at the next G8 meeting when the results of a research report would become available. Co-operation with industry was also emphasised at this meeting.

Ministers of G8 member-states met in Paris in May 2000 to develop their recommendations that ultimately became the final policy statement on cyber-crime that appeared at Okinawa.[3] The title of the meeting 'A Government/Industry Dialogue on Safety and Confidence in Cyber-space' revealed changing attitudes that the co-operation of the private sector was ever more important in tackling these complex issues. French President Jacques Chirac publicly opposed the creation of a US-backed international criminal force to deal with cyber-crimes; however, at the meeting, Chirac revealed a new French agency to do exactly the same.

Senior industry representatives, including executives from IBM, America On-line, Bell Atlantic, Citibank, Deutsche Telekom, MCI, and Microsoft met under the auspices of the Internet Alliance and presented a white paper as input into the process, presenting industry perspectives and suggestions.[4] Many argued that the most interesting aspect of this document was the presentation of the global and local consequences of cyber-terrorism and the need to incorporate national and local law enforcement authorities in any debate about Internet-based crime and terrorism. Effective law enforcement at all levels (local, national, and international) is needed to prevent gaps in coverage, gaps which could lead to overall ineffectiveness.[5]

Although the final *communiqué* emphasised the importance of the maintaining an overall ability to locate and identify Internet criminals through different systems, the document was also emphatic in proposing the creation of faster or more novel solutions (preferably implemented by a government and industry partnership) to deter, investigate, and prosecute 'crime that has an electronic component'. Such a solution would have to fulfil the following criteria: this would have to ensure the protection of individuals' freedoms and private life; preserve governments' ability to fight high-tech crime; facilitate appropriate training; and define a clear and transparent framework for addressing cyber-criminality and ensuring free and fair activities through the promotion of voluntary codes of conduct. However, industry were keen to point out at the meeting that ongoing Council of Europe proposals (such as the then-Draft Convention on Cyber-Crime) requiring ISPs to maintain records of user activity would be strongly unpopular.

All this preparation finally came to fruition at the July 2000 G8 summit in Okinawa and after two days of discussions, the Okinawa Charter on the Global Information Society. Prior to the Okinawa summit, experts from the G8 met in Tokyo to discuss the agenda on the table at Okinawa.

The Okinawa conference saw the release of the Okinawa Charter on the Global Information Society, which covered issues relating to the social, economic, and political consequences of the emerging information society. Among other things, the Okinawa Charter called for the application of the OECD 1992 guidelines on Information Security and also stronger public–private co-operation. Also suggested was that co-operation between other international organisations, such as the EU and UN should be improved.

---

[3] Background and general information about this conference at www.g8parishightech.org.

[4] *Ibid*.

[5] Internet Alliance, *An International Policy Framework for Internet Law Enforcement and Security – Internet Alliance White Paper* (May 2000): www.internetalliance.org/policy/leswp.html (downloaded 22 July 2000).

The main G8 policy statement regarding the development of an information society and knowledge economy comes in the form of the Okinawa Charter on Global Information Society. Broadly, the Charter says 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. By this statement, the G8 intends to exercise leadership in:

> …advancing government efforts to foster an appropriate policy and regulatory environment to stimulate competition and innovation, ensure academic and financial stability, advance stakeholder collaboration to optimise global networks, fight abuses that undermine the integrity of the network, bridge the digital divide, invest in people and promote global access and participation.

Both the public and private sectors are asked to make efforts to bridge the international information and knowledge divide. Efforts to develop a global information society should be backed by sound public-private partnerships and joint policy co-operation.

The G8 summit in Genoa in 2001 saw the publication of the DOT (Digital Opportunity Task Force – see below) report, *Digital Opportunities for All: Meeting the Challenge*, which contained what is known as the Genoa Plan of Action.

G8 Finance Ministers and Central Bank Governors met in early October in Washington, DC, to debate issues relating to terrorist financing, following the terrible events of 11 September 2001. The G8 urged the International Monetary Fund (IMF) and the Financial Stability Forum (FSF)) to accelerate their efforts to curb terrorist financing, particularly the use of the global financial system by ensuring adequate supervision in offshore financial centres and the provision of 'technical assistance' by the G8 to strengthen the integrity of offshore financial centres that are a favourite target of terrorist money laundering efforts. This is a clear statement of G8 desire to become involved with the confidentiality and information security debate central to the functioning of the banking system. An Action Plan to Combat Financing of Terrorism was subsequently published on 6 October.

Industry and Other Non-Government Activities Related to Dependability

Finally, the G8 suggested that their activities should be directed beyond the eight members to involve international or regional organisations such as the UN or the EU.

Public-Private Partnerships

The Okinawa Charter on Information Society asked (as discussed above) both the public and private sectors to make efforts to bridge the international information and knowledge divide. Efforts to develop a global information society should be backed by sound public-private partnerships and joint policy co-operation.

Finally, DOT – itself a public-private partnership comprising 43 teams from government, the private sector, non-profit organisations, and international organisations – was created by the G8 Heads of State at their Kyushu-Okinawa summit in July 2000. The aim of DOT is to provide co-operative efforts to identify ways in which the digital revolution can benefit all the world's people, especially the poorest and most marginalised groups. The 'digital divide' is threatening to exacerbate the existing social and economic inequalities between countries and communities, so the potential costs of inaction are greater than ever before.

Over several months, through a rich and unprecedented mix of plenary meetings, informal consultations, meetings with stakeholders, and electronic outreach to broader audiences across the world, DOT has examined in depth the challenge of bridging the digital divide and harnessing the

power of information and communications technologies (ICT) and global networks to assure opportunity, empowerment, and inclusion for all.

INTERPOL

Interpol – known formally as the International Criminal Police Organisation (ICPO) – was founded in 1923 with the aim to promote and facilitate enquiries into criminal activity. Headquartered in Lyon, France, Interpol acts in a co-ordinating capacity for the police forces of the 178 member-states.

The main areas of activity for Interpol are those crimes transcending international boundaries. These include offences against people and property; murder; kidnapping; offences involving cultural property; illicit trafficking in works of art or endangered species; economic and financial crime; counterfeiting; drug trafficking, and related offences such as money-laundering.

Also, Interpol has been actively involved for a number of years in combating Information Technology Crime. This has become a major concern for the organisation; in several media, Interpol calls for attention and immediate co-operation infighting escalating cyber-crime.[1]

Raymond Kendall, then secretary-general of Interpol, said in 2000 that his organisation is concerned that unlawful computer techniques are developing at such a rate that they represent a 'new phenomenon' for international law enforcers. Kendall urged international organisations not to wait for conventions to be passed before drawing up guidelines for a concerted response to the threat of cyber-crime.

Many of the 178 member-nations of Interpol are starting to draw up legislation to outlaw cyber-crime, but fewer than 15 of the member-nations currently have laws in place that criminalise malicious hacking or the spreading of destructive viruses.

'If we waited until the laws were adopted, we would wait a long, long time,' said Kendall. 'Unless we have the courage to step outside the usual run of the mill responses we will not achieve anything.' [2]

Law enforcement agencies currently lack the staff to investigate and prosecute most cyber-crimes - from break-ins to data destruction and theft to damaging viruses. As a result, cyber-criminals are breaking into or paralysing Web sites with little fear of retribution, costing the private sector hundreds of millions of euros.

Incidents like the release of the Lovebug virus and the distributed-denial-of-service attacks on major web sites are estimated to have cost businesses billions in damages. According to Kendall, Interpol is developing a new strategy for monitoring computer crime trends and working with the United Nations to assess ways to disseminate that information efficiently. Interpol is keen to see businesses - the principal victims of computer crime - share information with the service about computer attacks and vulnerabilities.[3]

---

[1] See for example: "The man from Interpol", CNN.com (27 June 2000): www.cnn.com/2000/TECH/computing/06/27/interpol.interview.idg/index.html; "New Interpol chiefs to tackle cyber-crime", CNN.com (3 November 2000): www.cnn.com/2000/WORLD/europe/11/03/interpol.bosses; "Interpol patrols the web", BBC (30 June 2000): news.bbc.co.uk/hi/english/sci/tech/newsid_812000/812764.stm; Will Knight, "Interpol orders immediate cyber-crime action", ZD Net UK (11 October 2000): news.zdnet.co.uk/story/0,,s2081907,00.html

[2] "Interpol patrols the web", BBC (30 June 2000): news.bbc.co.uk/hi/english/sci/tech/newsid_812000/812764.stm

[3] Will Knight, "Interpol orders immediate cyber-crime action", ZD Net UK (11 October 2000): news.zdnet.co.uk/story/0,,s2081907,00.html

Also, Ronald K Noble, who replaces Kendall as Interpol's secretary-general, said cyber-criminals should now be a central focus of international policing as they caused untold damage at little cost to themselves and crime fighters were struggling to keep up with them: 'The technology is light-years ahead of the legislation and the police know-how.'

According to Noble, there are two main types of Internet crime: the theft of intellectual property and cyber-crime, epitomised by high-profile virus attacks on worldwide computer systems.

One problem with fighting cyber-crime, particularly virus attacks, is that not all countries have relevant laws to enforce. 'There hasn't been a database established for what laws exist or a structure for police to work together,' Noble said, adding Interpol would now work to correct this.

The Interpol general assembly endorsed making Internet crime a key priority, along with tackling the trafficking of women and stamping out police corruption.[4]

To counter cyber-crime, Interpol developed several strategies. One of these is co-operation and communication between itself and national- and international-level law enforcement and intelligence agencies, already in existence for the more traditional fight against international crime.

More recently, efforts have been made to establish public-private partnerships, between Interpol and members of the high-tech business sector. This is also needed because of the limited knowledge among its personnel, scarcity of resources, and the fundamental new problems posed by cyber-crime.[5]

Interpol currently has about a half-dozen investigators devoted to Internet crime.

Information Technology Crime (ITC)

To help companies and governments cope with the rising tide of cyber-crime, about a decade ago Interpol established the 'Information Technology Crime' (ITC) group. Starting with a working group at the European level, later further regional working parties were created representing the African, American, and Asian regions.[6]

All regional working parties are subject to a Steering Committee, made up of representatives from the various regional working parties, responsible for co-ordinating the projects and efforts of the working parties. The Steering Committee's main functions are to ensure that there is no unnecessary duplication of efforts and to seek proposals to harmonise legislation, investigative skills, and training techniques. The Steering Committee met for the first time in October 1997, with representatives from the American, English-speaking Asian, and European regions present.

---

[4] New Interpol chiefs to tackle cyber-crime", CNN.com (3 November 2000): www.cnn.com/2000/WORLD/europe/11/03/interpol.bosses/

[5] Rathmell and O'Brien, *Information Operations: An International Perspective.*

[6] At the 19th European Regional Conference in Budapest (1990), it was decided that a group of experts should be established to deal with computer-related crime. The European Working Party on Computer Crime was originally composed of representatives from Belgium, Finland, France, Germany, Italy, the Netherlands, Spain, Sweden, and the United Kingdom. The 25th European Regional Conference, held in Warsaw in 1996, changed the name of the working party to European Working Party on Information Technology Crime and established the terms of reference for the group. In accordance with the Resolution AGN/64/RES/22, adopted at the 64th General Assembly Session (Beijing 1995), and implemented by the 2nd International Conference on Computer Crime, held at the General Secretariat in May 1996, further regional working parties were to be created representing the African, American, and Asian regions.

The working party consists of the Heads or experienced members of national computer crime units. These working parties have been designed to reflect regional expertise and exist in Europe, Asia, the Americas, and in Africa. All working parties are in different stages of development.[7]

Besides the regional working parties and the steering committee for Information Technology Crime, on Interpol's website, items can be found on information security and crime prevention (including a report called 'IT Security and crime prevention methods')[8], a company and private checklist, and a part on virus alerts.[9]

From all these initiatives, the European working party on Information Technology Crime is one of the most noteworthy contributions to date.

The European Working Party on Information Technology Crime

The European Working Party on Information Technology Crime[10] was formed in 1990 and has since then met three times a year; in January 2001 the Secretariat hosted the 30th meeting of the working party, currently represented by members from Belgium, Finland, France, Germany, Italy, the Netherlands, Spain, Sweden, and the United Kingdom. The General-Secretariat representative from the Economic Crime Branch fulfils the role of Secretary of the working party (WP).[11]

According to the terms of reference, the aims of the Working Party are:[12]

- Co-operation; sharing of knowledge and practical experiences to discuss information technology crime; find solutions to the problems that arise and propose recommendations with a view to assisting Interpol member-countries to prevent, detect, and combat such crime;

- Promotion of standardisation of methods and procedures, special projects, training programs, and co-operation with other international organisations; and

- To establish good practice guidelines for relevant investigations and make them available to the Interpol member-countries (Computer Crime Manual).

Activities of this Working Party include:

---

[7] www.interpol.int

[8] See www.interpol.int/Public/TechnologyCrime/CrimePrev/ITSecurity.asp

[9] Especially this last section has been criticised. After reviewing the new security section on Interpol's site, many security experts said the agency had simply cobbled together a superficial overview of security issues and had not provided any truly useful information to help businesses and governments combat viruses or attacks by malicious hackers. But some experts felt that the agency's effort should be applauded, even if the site isn't as useful as it could be. The value that Interpol has may be more in the creation of awareness rather than having the most up-to-date information on the latest threat. Michelle Delio, "Interpol's Virus Site Too Fluffy?", WIRED (15 May 2001): www.wired.com/news/politics/0,1283,43787,00.html

[10] See www.interpol.int/Public/TechnologyCrime/WorkingParties/Default.asp#europa

[11] The current Chairperson is Robert Jones from the Queen Mary and Westfield College, University of London; the Vice-Chairperson is Eric Freyssinet, Head of the Computers and Electronics Department, Institut de Recherche Criminelle de la Gendarmerie Nationale, Paris; the third board member is Jukka Mäkynen, CISSP, National Bureau of Investigation, Computer Crime Squad, Vantaa, Finland.

[12] Interpol – Revision, 31st Meeting (24-26 April 2001): www.interpol.int/Public/TechnologyCrime/WorkingParties/Default.asp#europa

- The compilation of a handbook on the investigation of computer-related crime, which serves as an introduction for a novice;

- The compilation of the computer crime manual, a best-practise guide for the experienced investigator, which is continually updated. The manual is available on CD-ROM and the content will be digitally available via the Interpol website;

- The WP has, for the past five years, presented numerous training courses in order to share expertise with other members; these training courses are cost-efficient and can target different levels of expertise and subject-areas, ranging from introductory courses to courses specialising in Internet investigations; four courses are scheduled for 2001 to be held in France, Germany, Finland, and Italy;

- The WP has also designed and implemented an early-warning system that essentially consists of three elements: an international 24-hour response system, National Central Reference Points (listing responsible experts within each of the 61 countries currently participating), and a formatted Computer Crime message format (to ensure that all the essential information is transmitted);

- The WP also recognised the necessity to complement its knowledge with outside expertise; 'project groups' are specific task-motivated groups led by WP members who, within the framework of a specific set period, have to complete their project (the meetings are merely used to co-ordinate and streamline the efforts by the individuals; the real work is done on their own time; this has proven to be a very successful and time efficient method);

- Projects. In 1998, three projects were completed dealing with 'the Internet', 'Electronic Means of Payment', and 'Manipulation of Public Communication Networks'; a further four projects were completed in 1999, namely 'IT Crime Prevention', 'Tools and Techniques as an aid to the Investigator', 'Internet Investigations', and an 'Internet Investigation Training Exercise'. Projects for the year 2000 included the IT Crime Training: 'Train the Trainers' (held from 22-26 January 2001 in Ecully, France); 'Criminal Threats against E-Commerce' (CTEC; Tools and techniques 2; Internet investigations 2; and a training video for international law enforcement). Projects for 2001 include training (development of three modules focusing on investigation - entry level, a module for senior management, a module for Local Area Network (LAN) managers); compile best practices on digital evidence; 'wireless technology' - threat assessment of evolving technologies; definition and statistics - setting standards for the European region to serve as model for other regions; revision of Computer Crime Manual; and Internet Investigations 3.

The Interpol Network and Other IT Activities

Roughly 20 percent of Interpol's annual budget of US$30 million (€34.5 million) is devoted to information technology. As explained by Peter J. Nevitt, director of IS at Interpol, the organisation has a network linking 178 countries and the Interpol general-secretariat. Through that network, two kinds of services are offered. The first is an email service. Country A sends a message to country B asking for assistance or co-operation. Country B replies. During 1998, 2.4 million messages went through that network.[13]

[13] "The man from Interpol", CNN.com (27 June 2000): www.cnn.com/2000/TECH/computing/06/27/interpol.interview.idg/index.html

Interpol also provides access to an international database of criminal information – including wanted criminals, missing persons, organised crime groups, drug seizures, unidentified dead bodies, and stolen artwork. So countries use email to send information to the general-secretariat, who incorporate data into the international database and then make that database available to every country in the world or to those countries deemed appropriate by the owner of the information.[14]

Internet technologies are used in three ways. The first is a public relations website, with simple, non-sensitive police information directly to the public. The second is a secure domain of the site with restricted information that helps investigators do their jobs. The third use of Internet technologies is to replace the X.400 network with a secure IP network.

Interpol is a member of the Information Security Forum, a co-operative group of some of the major European companies and government organisations that share expertise on security and develop and apply standards.[15]

EUROPOL

Europol – the European Police Force – is the European Union law enforcement organisation that handles criminal intelligence, whose aim is to improve the effectiveness and co-operation between the competent authorities of the member-states in preventing and combating serious international organised crime.[16]

The establishment of Europol was agreed to in the Maastricht Treaty on European Union of 7 February 1992. Based in The Hague, Europol started limited operations on 3 January 1994 in the form of the Europol Drugs Unit (EDU). Progressively, other important areas of criminality were added. The Europol Convention was ratified by all member-states and came into force on 1 October 1998. Following a number of legal acts related to the Convention, Europol commenced its full activities on 1 July 1999.

According to the Council Act of 26 July 1995, drawing up the Convention on the Establishment of a European Police Office (Europol Convention), Europol has as principal tasks to facilitate the exchange of information between member-states, and to obtain, collate, and analyse information and intelligence.

To perform its tasks, Europol maintains a computerised information system. Data are directly entered into the system that is directly accessible for consultation by national units, liaison officers, the Director, the Deputy Directors, and duly empowered Europol officials.

---

[14] Peter J. Nevitt on how Interpol moved into the IT area: "We began design of a global telecommunications network in the early '90s. In 1994, we began rolling it out to the world, an X.400 network running over X.25 lines. The rollout was finished only last year. The problem was that only one-quarter of the countries could afford the equipment and the line. So Interpol raised money from its richer members and from other organisations, such as the United Nations, to fund the leased lines, install the equipment, and provide training in 130 of its 150 member countries. Interpol was one of the first major global organisations to contract with SITA, which is now Equant NV, a private company created and owned by a consortium of airline companies that collaborated to develop a global network for ticket reservations, air traffic control and so on, to act as network operator and to install and maintain the equipment": "The man from Interpol", CNN.com (27 June 2000): www.cnn.com/2000/TECH/computing/06/27/interpol.interview.idg/index.html

[15] "The man from Interpol", CNN.com (27 June 2000): www.cnn.com/2000/TECH/computing/06/27/interpol.interview.idg/index.html

[16] Including terrorism, drug-trafficking, trafficking in human beings, crimes involving clandestine immigration networks, trafficking in radioactive and nuclear substances, vehicle trafficking, combating the counterfeiting of the euro, and money-laundering associated with international criminal activities.

The information system may be used to store non-personal data and personal data. The creation of a computerised personal data file by Europol is subject to an instruction approved by the Management Board. Personal data retrieved from the information system can only be transmitted or used by the competent services of the member-states to prevent and combat crime coming under the competence of Europol, and other serious criminal offences. [17]

The Europol Information System

The initial work on the information system started last year with a series of workshops and expert meetings resulting in the production of a detailed specification, which had been approved by the Management Board in December 2000. The contractual arrangements for the next step, the actual development of the information system, were negotiated and agreed to, allowing this work to commence in January 2001. The Europol information system is being developed by a consortium headed by EADS-Sycomore, with DataMat and Saillabs. The system will provide for the first time a multilingual European platform to store and retrieve information on criminals, scenes of crimes, criminal organisations, and *modus operandi* that can be accessed by all member-states. The aim is to provide a 'real time', up-to-date overview on organised crime within and affecting the European Union.[18]

Europol Mandate Concerning Cyber-crime

In October 2000, the French Presidency tabled a proposal for the extension of Europol's mandate to the fight against cyber-crime for the council of the European Union.[19] According to this proposal, Europol should be entrusted with new responsibilities, centred on an extension of Europol's mandate to computer crime.

The possibility of Europol's involvement in fighting cyber-crime had already been mentioned in the Europol treaty. According to France, the new role of Europol is intended 'first and foremost' to be pragmatic and to provide a basis for an 'operational response to the problems involved in combating cyber-crime'. Attacks on automated data-processing systems - creating and spreading viruses, breaking in, altering or interfering with the operation of a system, altering or modifying data - fall outside the scope of Europol's mandate.[20] France therefore wants to extend Europol's mandate to these kinds of attacks.

The official definition of computer crime in this context will be 'all forms of attack on automated data-processing systems'.

---

[17] europa.eu.int/scadplus/leg/en/lvb/l14005b.htm. See for more details on the Europol Convention: europa.eu.int/eur-lex/en/lif/dat/1995/en_495A1127_01.html

[18] www.europol.eu.int/home.htm?home/en.htm

[19] Council of the European Union, *Proposal for the Extension of Europol's Mandate to the Fight Against cyber-crime – Note from Presidency* (12 October 2000): www.xs4all.nl/~respub/europol/cyberpol.html. See also Jelle van Buuren, "European Commission Wants To Tackle Cyber-crime" (10 January 2001): www.heise.de/tp/english/special/enfo/4658/1.html

[20] Offences relating to new technology are usually divided into three categories: 1) attacks on automated data-processing systems (e.g., creating and spreading viruses, breaking in, altering or interfering with the operation of a system, altering or modifying data); 2) traditional offences committed by means of new technology which carry the same penalties as if they had been committed by more traditional means (e.g., money-laundering, drug trafficking). In such cases, it is not the content carried which is in itself illegal, but the offence to which it relates; and 3) offences inherent in the content carried by new technology (e.g., child pornography, racism, infringements of intellectual property). In these cases, the illegality lies in the content itself. The first category of offences connected with new technology – attacks on automated data-processing systems – is not covered by Europol's present mandate and requires the mandate's extension. (Council of the European Union, *Proposal for the Extension of Europol's Mandate to the Fight Against cyber-crime – Note from Presidency* (12 October 2000): www.xs4all.nl/~respub/europol/cyberpol.html

Yet, to date and according to the Europol convention, cyber-security is not a mandated area of the organisation. Only when related to other mandated areas of international crime are activities in this field employed.

However, cyber-crime has some implications with crime already within the mandate, like terrorism, child pornography, and smuggling in human beings. According to Paulo Felix, intelligence analyst at Europol, cyber-crime is interwoven with other kinds of organised crime; organised crime using telecommunications or advanced technology as a means to achieve goals. Just like the rest of the business world, organised crime is learning ways to use the Internet to streamline its processes and increase profit margins.[21]

Within the organised crime department of Europol, different types of crimes are analysed, including the implications that the use of computers may have or are already having on criminal organisations and how they do business.[22]

Also, in the last couple of years, several meetings were organised on computer crime and information security. After expert meetings in 1999 and 2000, in March 2001, Europol held its first Internet Crime Expert Working Group meeting, with a second follow-up meeting more recently.

During one of these meetings, the need was expressed for trust from the private sector in order to be able to get the information needed for further investigation. Most victims of cyber-crime are companies in the private sector. Without their reports of the crimes being committed, there is no information on which Europol can work. According to Paulo Felix, 'trust and relation with the private sector is fundamental for us at Europol to be able to tackle these new threats.'[23]

So although Europol does not officially investigate cyber-crimes, the topic is getting more attention and may yet become a major issue in the future if the political decision is made and the mandate given. Also, in November 2001, Interpol and Europol signed a co-operation agreement. Hopes are good that such a move to share critical criminal intelligence will strengthen the work of both organisations, especially when it comes to organised crime like cyber-crime.[24]

---

[21] "Inside Europe's cybersleuth central", MSNBC: www.msnbc.com/news/481681.asp?cp1=1#BODY. See also personal conversation with Paulo Felix, Intelligence Analysis Department Europol**,** 26 November 2001 (IG)

[22] Paulo Felix (Europol), *Cyber Security Conference: A Transatlantic Perspective*. Sponsored by RAND Europe, Royal Dutch Shell Company, and the US Embassy (Netherlands). The Hague (9 April 2001).

[23] Felix, *op cit.*.

[24] "Interpol and Europol sign co-operation agreement". Interpol Press Release (5 November 2001): www.interpol.int/Public/ICPO/PressReleases/PR2001/PR200133.asp

INTERNATIONAL TELECOMMUNICATIONS UNION (ITU)

The International Telecommunications Union (ITU) – an intergovernmental organisation – involves both public and private actors, and develops international regulations and treaties governing the use of the frequency spectrum within which countries adopt their national legislation. ITU also drafts standards to facilitate the global interconnection of telecommunication systems, while fostering the expansion of these services through medium-term policies and strategies. In light of the growing convergence between information and telecommunication services, the ITU is playing an increased role in promoting e-commerce – and, increasingly into the future, network security.

Socio-Political, Economic, and Commercial Overview

The ITU is headquartered in Geneva, Switzerland, within which governments and the private sector co-ordinate global telecom networks and services.

The ITU as a whole is overseen by a Council (the annual governing body of the Union), and a General-Secretariat. The work of the ITU is organised into three sectors:

- The Radiocommunication Sector (ITU-R) consists of the Radiocommunication Bureau and is informed by World/Regional Radiocommunication Conferences and Assemblies, the Radio Regulations board, and advisory and study groups. The Sector's role is in the management of the radio-frequency spectrum and satellite orbits.

- The Telecommunication Standardisation Sector (ITU-T) consists of the Telecommunication Standardisation Bureau and is informed by the World Telecommunication Standardisation Assemblies, as well as advisory and study groups. The ITU-T produces standards concerning all fields of telecommunications

- The Telecommunication Development Sector (ITU-D) consists of the Telecommunication Development Bureau and is informed by World/Regional Telecommunication Development Conferences, as well as advisory and study groups.[1]

The ITU holds Plenipotentiary conferences as well as the World Conferences on International Telecommunications. The Plenipotentiary Conference is the main policy-making body of the ITU. The Conference is held every four years and sets the Union's general policies, adopts five-year strategic and financial plans, and holds elections.

The focus of the ITU is the assurance of quality and the enabling of effective use of telecommunication technologies. To this end, there are many study groups and services that cover specific topics with security implications, such as: Wireless Access System (WAS), Broadcasting-Satellite Service (BSS), Mobile satellite services (MSS-RNSS), Satellite news-gathering (SNG), Optical Networks, Quality of Service, Telecommunication management, Signalling requirements and protocols, IP, and Global Information Infrastructure.[2]

There are many ITU initiatives that specifically deal with cyber-security and a few will be discussed in later sections. In general, the ITU seems only recently to be focusing on these issues; most specific initiatives date back only two-three years. For example, the ITU Council decided, on 28

---

[1] Structure of the ITU: www.itu.int/aboutitu/structure/index.html

[2] ITU Homepage, www.itu.int

July 2000, to proceed with the preparation of the first World Summit on the Information Society, to be held in 2003 in co-operation with the United Nations. The goal of the conference is the making of a strategic plan of action for issues concerning the realisation of a true information society.[3] This recent focus on more social aspects of telecommunications (such as security, access, crime, and development) could be the result of the reform of the ITU that began in 1999 and called for a review of the ITU's rights, obligations, management, functioning, and structure.[4]

Analysis of the Main Regulatory and Legal Developments Related to Information and Telecommunication Systems and Services

Economic and industrial environment affecting state control of key industries: The ITU stresses international co-operation between governments and the private sector. To this end, the ITU aims to help government and industry work towards consensus on a wide range of issues affecting communications technologies. ITU member-states and sector members have access to a number of services including the Telecommunication Information Exchange Service (TIES) and ITU's Who's Who.[5]

Government-led initiatives for expanding access to the Internet and other information infrastructures and services: Facilitating connectivity and access to the Internet is a stated goal of the Telecommunications Development Sector of the ITU (ITU-D). Activities of the ITU-D concerning the expansion of access are focused around the Valetta Action Plan Programme 3, which began in 1998. The objective of the VAP Programme 3 is to develop best-practice, sustainable, and reproducible models of ways to provide access to ICT, particularly to people in rural and remote areas. The ITU-D undertakes pilot projects in a number of countries in different regions, at different stages of development, and with different geographical, social, economic, and cultural conditions in order to reach the VAP goals.[6]

Government-led initiatives aimed at fostering electronic commerce: The ITU's work on harmonisation and standardisation of electronic information is in part stimulated by the demands of e-commerce. Relevant recommendations and resolutions concerning electronic security are covered in 'Organisational initiatives aimed at tackling cyber-security/cyber-crime...' below.

A recent initiative regarding electronic commerce has been developed by the Electronic Commerce for Developing Countries (EC-DC) program of the ITU-D. The EC-DC has developed an electronic certification and authorising system, the Public Key Infrastructure (PKI), which has already been tested and is now fully operational. By using PKI, certified users from both developing and industrialised countries 'will be able to communicate securely, conduct business transactions in a secure and trusted manner and run other e-services such as e-government, e-health and e-learning.' The core body of the PKI is the 'E-commerce PKI Certification Authority.'[7]

General legal principles and developments related to the ICT environment; overview of relevant new legislation: This is a main function of the ITU. Developments of note will be covered in 'Organisational initiatives aimed at tackling cyber-security/cyber-crime…' below.

---

[3] The World Summit on the Information Society: www.itu.int/wsis/brochure.htm

[4] Reforming the ITU: www.itu.int/newsroom/reform/index.html

[5] ITU Overview: www.itu.int/members/index.html

[6] ITU, *Rural Development and Universal Access*: www.itu.int/ITU-D/univ_access/reports/PPstatus981016.html

[7] Electronic Commerce for Developing Countries: www.itu.int/ITU-D/ecdc/index.html

Assessment of Phenomena Undermining Dependability

The ITU makes few explicit statements on cyber-crimes, but does widely emphasize the importance of security and integrity of information systems. Worth noting is the ITU's initiative on Critical Network Infrastructures, which was formed to address issues of vulnerability. The ITU consistently identifies the phenomena that brought about the formation of the Critical Network Infrastructures initiative in this excerpt from its mission statement: '[the rise of] hostile attacks on infrastructure by network predators. Newly discovered forms of attacks, the availability and wide distribution of attack tools, as well as the flaws in common desktop software … Simple viruses are argued to have cost billions of dollars worldwide in lost productivity. Sophisticated distributed denial of service attacks on the Internet are on the rise.'[8]

Organisational Initiatives Aimed at Tackling Cyber-Security/Cyber-Crime or Assisting with the Development of Dependability

The ITU maintains a catalogue of security-related Recommendations listing 59 approved measures and five other draft recommendations. Examples include:

1. Recommendation X.842 'provides guidance for the use and management of Trusted Third Party (TTP) services';

2. Recommendation X.841 regarding Security Information Objects (SIOs) for Access Control 'provides object definitions that are commonly needed in security standards to avoid multiple and different definitions of the same functionality.'

3. Recommendation F.851, providing 'the service description and operational provisions for Universal Personal Telecommunication (UPT).'

4. Recommendation H.235, covering security and encryption of 'real-time communication over insecure networks'.

5. Recommendation H.323, describing 'terminals and other entities providing real-time audio, video, data and/or multimedia communications services over Packet Based Networks (PBN) which may not provide a guaranteed Quality of Service.'

6. Recommendation T.36, which 'defines the two independent technical solutions which may be used in the context of secure facsimile transmission.'[9]

Central policy and operational co-ordination mechanism: The ITU-T routinely forms Lead Study Groups (LSGs) for studies forming a defined programme of work involving a number of Study Groups. Study Group 7 has been designated the LSG for Communication Systems Security (CSS). The core activities of the Study Group 7/CSS-LSG involve the definition and maintenance of security frameworks and the management of project activities involving the co-ordination, assignment, and prioritisation of efforts that would lead to timely communication system security Recommendations. The LSG-CSS works closely with other ITU Study Groups to identify and develop security solutions. However, the LSG-CSS will not have a planned role in the development and registration of specific cryptographic algorithms (ISO performs this function), nor in the certification of security systems. A major contribution of the LSG-CSS is a catalogue of security-

[8] ITU, *Critical Network Infrastructures*. www.itu.int/osg/spu/ni/security/index.html

[9] *Catalogue of ITU-T Recommendations Related to Communication Systems Security:* www.itu.int/itudoc/itu-t/com7/sg-acti/cat001.html

related Recommendations, as well as Terms and Definitions of the ITU.[10] The compendium is currently a work in progress and is open to comments and alterations. The intent of the catalogue is to help those who need to incorporate security features into their products or wish to know about ITU's progress on security.[11]

Government-sponsored schemes aimed at enhancing the security of information and network systems: The ESCA (Electronic Signatures and Certification Authorities) working group has discussed Information Security and Assurance.[12] ESCA activities build upon previous ITU work in the field of standardisation. In December 1999, ESCA held a first meeting to structure the ITU's role in enhancing authentication in an e-commerce environment. The meeting involved over thirty experts from governments, law firms, academia, e-commerce, and standards managers of telecommunication carriers and manufacturers, as well as ISPs. Participants emphasized the ITU's unique position for the harmonisation of national legislations and regulations due to its global membership. Still, the ITU was invited to keep in mind the needs of the telecommunication companies, as well as of users, in defining common and standardised approaches to online authentication through electronic signatures. The objective was to devise the necessary instruments to establish trust over the Internet and its associated information and network technologies. This can only be achieved by establishing:

> confidence that on-line purchases, funds transfers, and business deals will be as valid as traditional activities and that the world of on-line commerce and communication will be at least as accountable for the quality, reliability, and legality of products and services as is the in-person world.[13]

Nevertheless, differently from UNCITRAL (see 'United Nations'), ESCA decided to espouse a completely technologically-neutral approach, inviting the ITU:

> not to impede the development and implementation of market-based initiatives and standards and of private arrangements, while being particularly attentive to the needs of developing countries, cultural difference among individuals and groups, and both the potential risks and opportunities presented by the various authentication measures for economic, infrastructure, and social development.[14]

Finally, this group invited the ITU to continue one of its pivotal functions as an international organisation with global membership: education and training. Technologies related to electronic signatures and authentication require an in-depth understanding of their legal, technological, and managerial characteristics. In light of the Internet's global span, every country needs to acquire the necessary expertise; the ITU can provide this by structuring education and training initiatives. In particular, the ITU should facilitate the 'exchange of information within the telecommunication industry and between this sector and other industries about their experience with authentication'.[15]

---

[10] *Catalogue of ITU-T Recommendations Related to Communication Systems Security*: www.itu.int/itudoc/itu-t/com7/sg-acti/cat001.html

[11] *Communications Systems Security*: www.itu.int/ITU-T/studygroups/com07/cssecurity.html

[12] For a description of its activities, see the ESCA's website at www.itu.int/osg/sec/spu/ni/esca/index.html.

[13] Stewart Baker and Matthew Yeo, "Background and Issues Concerning Authentication and the ITU", Paper presented at the ITU-Expert Meeting on Electronic Signatures and Certification Authorities: Issues for Telecommunications, 9-10 December 1999, Doc. n.2 (16 November 1999): available at www.itu.int/osg/sec/spu/ni/esca/meetingdec9-101999/briefingpaper.htm (downloaded 29 May 2000).

[14] "High-level Experts Recommend Framework for ITU's Role in Authentication for E-Commerce", ITU Press Release ITU/99-26 (17 December 1999): available at www.itu.int/newsarchive/press/releases/1999/99-26.html (downloaded 29 May 2000).

[15] *Ibid.*

Regarding certification and accreditation, a recent initiative aimed at supporting electronic commerce has been developed by the Electronic Commerce for Developing Countries (EC-DC) program of the ITU-D. The EC-DC has developed an electronic certification and authorising system, the Public Key Infrastructure Key (PKI). For more detail on the PKI, see above "Government-led initiatives aimed at fostering electronic commerce".

Government schemes aimed at fostering the use of dependability-enhancing technologies and services: Many of the current standards on electronic authentication, digital signatures, and certificates are based on ITU global telecommunications recommendations, notably ITU-T Recommendation X.509, which covers data networks and open-system communication.[16]

The ITU has recently adopted two draft new global standards for increasing the efficiency and survivability of optical fibre access networks based on Passive Optical Network (PON) techniques. The draft new standards are designated ITU-T Recommendations G.983.4 and G.983.5. 'The draft new standard G.983.4 specifies a Dynamic Bandwidth Assignment (DBA) mechanism which improves the efficiency of the PON by dynamically adjusting the bandwidth among the Optical Network Units (ONUs) that are near end users or in homes, for example, in response to high-volume traffic requirements.' The benefits of this approach are that network operators are able to add more users to the PON due to increased efficiency and that users are able to use service requiring large bandwidth. The draft new standard G.983.5 'specifies a number of protection options for PONs which will enable enhanced survivability for e.g., Fibre To The Cabinet (FTTCab) and the delivery of highly reliable services in the case of e.g., Fibre To The Office (FTTO).' The new draft standards for the G.983.3 standard allowed for an additional wavelength band to the downstream direction of a Broadband—Passive Optical Network (B-PON) which permits separate wavelengths for interactive and broadcast services over an optical distribution network.[17]

In January 2002, the United Nations announced the formation of a World Summit on the Information Society to 'address the digital divide' in order to 'harness the development potential of ICT'.[18] The Summit, expected to promote access by all countries to information, knowledge, and communications technologies for development, is to be held in two phases: the first in Geneva in 2003 and the second in Tunisia in 2005 and is being convened under the high patronage of the UN Secretary-General, Kofi Annan. The ITU will be taking the lead role in Summit preparations, in co-operation with other interested organisations and partners. Resolution A/RES/56/183 calls on governments to participate actively in Summit preparations and to be represented at the highest possible level. The resolution has also asked for the active participation and effective contribution in the Summit and its preparations by all relevant United Nations and intergovernmental organisations, including international and regional institutions, as well as non-governmental organisations, the civil society, and the private sector. The ITU will work to create synergies and develop co-operation among the various ICT initiatives at the regional and global level.

The World Summit on the Information Society is an initiative of the 1998 Plenipotentiary Conference of ITU and is being endorsed by the General-Assembly as an effective means to assist the United Nations in fulfilling the goals of the Millennium Declaration - the landmark document adopted by a record number of leaders when they met during the Millennium Summit to address the key challenges of our time. Secretary-General Kofi Annan states: 'the Millennium Summit recognised the key role of partnerships involving governments, bilateral and multilateral

---

[16] Data Networks & Open System Communication: www.itu.int/rec/recommendation.asp?type=productsandparent=T-REC-x

[17] ITU Press Release: "Bringing broadband to the home: more steam for Internet access" (19 November 2001): www.itu.int/newsroom/press_releases/2001/27.html

[18] ITU Press Release (9 January 2002): www.itu.int/newsroom/press_releases/2002/UNGA_res_56_183.html

development agencies, the private sector and other stakeholders in putting ICTs in the service of development.' The General-Assembly has also invited the international community to make voluntary contributions to a special trust fund established by the ITU to support the Summit, as well as to facilitate the effective participation of representatives of developing countries, in particular those from the least-developed countries (LDCs).

The proposed themes of the Summit, addressing the central issues raised by the Information Society, will likely include:

- Building the infrastructure
- Opening the gates: universal and equitable access to the information society
- Services and applications
- The needs of the user
- Developing a framework
- ICT and education

Under each of these broad themes, consideration will be given to the relevant developmental, economic, policy, social, cultural, and technological aspects. A series of preparatory meetings will be held in 2002, beginning with the first PrepCom in Geneva from 1-5 July 2002.

Government schemes to assess the threat or to provide warnings and response capabilities to government or private sector clients: Within the ITU's New Initiative Programme, a new project has been formulated: the Critical Network Infrastructures. The initiative is looking past preventive measures or patches and towards more upstream identification of ICT infrastructures that are vulnerable. Proposed topics of consideration include the architecture of the Internet, the costs in terms of users' loss of confidence, increasing global awareness of the issues, global security monitoring, policy considerations, risk management strategies, the respective roles of the private sector and government, and approaches towards protecting critical network infrastructure.

The ITU will be organising a New Initiatives workshop on the subject of network security in May 2002, to be hosted by the Republic of Korea. The workshop will focus on the security, availability, and public trust of underlying network infrastructures. Topics to be considered will include the role of regional and international organisations, the 'definition of terms of reference with regards to critical network infrastructures, the need for a global, international approach to the dissemination of information regarding the security of critical network infrastructures and ways to stimulate international and regional co-operation with respect to critical network infrastructure.'[19]

Industry and Other Non-Government Activities Related to Dependability

The ITU does have industry bodies as part of their membership; however, activities undertaken by the ITU are not differentiated between governmental and non-governmental.

---

[19] *Creating Trust in Critical network Infrastructures*: www.itu.int/osg/spu/ni/security/index.html

Public-Private Partnerships

The ITU was 'founded on the principle of international co-operation between government and the private sector,' so the entire organisation is essentially a Public-Private Partnership (PPP); ITU membership includes over 650 Sector Members and only 189 member-states.[20] Recent examples of more overt PPP's include:

1. The signing of a memorandum of understanding (MOU) with Cable and Wireless Virtual Academy (CWVA) aimed at training opportunities LDCs via remote learning for telecommunication professionals in LDCs. Expectations are that in the year 2002 the allocations will benefit 30 LDC candidates selected by ITU for postgraduate degrees in Communications Management and in Law. Additionally, over 100 users are expected in short-term courses such as 'Regulations and Policy in Communications', 'Introduction to IP Technology for Business,' 'Managing Partnerships,' and 'Managing in the Virtual Organisation.'[21]

2. The signing of a non-exclusive MOU with Siemens and Alcatel within the framework of the Centres of Excellence Initiative. The two European manufacturers will make in-kind contributions in equipment and make their experts available to train the trainers. Training at the ITU Centres of Excellence is provided to policy-makers, regulators, high-level corporate managers, and frequency managers.[22]

[20] ITU Overview: www.itu.int/members/index.html

[21] ITU Press Release: "ITU and Cable and Wireless Team Up to Deliver Training to Least Developed Countries" (15 November 2001): www.itu.int/newsroom/press_releases/2001/25.html

[22] ITU Press Release: "Alcatel and Siemens Boost ITU's Centre of Excellence Initiative" (14 November 2001): www.itu.int/newsroom/press_releases/2001/23.html

NORTH ATLANTIC TREATY ORGANISATION (NATO)

Overview

Within NATO, information operations (IO) have been a working group of the military staff since 1997. Following a symposium held in December 1997, NATO approved an initiative for information operations in May 1998. In December of that same year, the North Atlantic Council followed suit by approving a NATO information operations policy. While an IO policy was now in place, extensive inclusion of IO in NATO planning and exercises did not take place until after 1999. A heightened focus on information operations and dependability arose due to NATO's involvement in the Kosovo conflict in 1999. At the conclusion of NATO's Operation Allied Force, Admiral first name Ellis deemed that effective use of IO 'could have halved the length of the campaign.'[1]

Information operations for NATO are handled on the most basic level by the NATO CIS Operating and Support Agency (NACOSA), which provides operational support to the Alliance in the form of hardware and software maintenance, personnel training, installation and security services for authorised users.[2] Informing this body and NATO's other information activities in regards to recognised threats and defence is the NATO Consultation, Command, and Control Agency (NC3A) and its organisation. The Research and Technology Organisation (RTO) of NATO also plays a large role in this area by identifying subjects concerning information security, dependability reviews, and recommends the establishment of research and development initiatives in these fields. NATO's Parliamentary Assembly (NATO-PA) provides a critical forum for international parliamentary dialogue on an array of security, political, and economic matters, including information technology, aimed at fostering mutual understanding among NATO parliamentarians. Smaller bodies within NATO dealing with different aspects of information security and dependability can be found in the following text.

Analysis of the Main Regulatory and Legal Developments Related to Information and Telecommunication Systems and Services

The **Agreement between the Parties to the North Atlantic Treaty for the Security of Information** outlines the rules for the 'reciprocal protection of classified information produced by, or released to, NATO.' The agreement also establishes common standards for security clearance amongst the Allied countries for the security of shared information. The security arrangements of co-operative activities such as this, which are approved by the North Atlantic Council, are the responsibility of the NATO Office of Security (NOS), who in turn liases with the NATO Security Service to further ensure the security of disclosed information and will ensure that any information disclosed will receive satisfactory protection.[3]

The NATO Headquarters **Information Systems Service (ISS)** provides information systems support to the North Atlantic Council, the Defence Planning Committee, the Military Committee, subordinate committees, and supporting staff. The ISS also offers systems design, development and maintenance support to NATO's International Staff and to the Military Agency for Standardisation. The role that ISS plays in the security and dependability of the NATO

---

[1] Rathmell and O'Brien, "North Atlantic Treaty Organisation", *Information Operations: An International Perspective.*

[2] NATO Handbook. www.nato.int/docu/handbook/2001/hb140806.htm

[3] *Explanatory Memorandum for the NATO Security of Information Agreement* – signed 29 September 1998. UK Foreign and Commonwealth Office. Paper #: 4787 S: www.fco.gov.uk/text_only/directory/expmemtxt.asp?Id=158andfco.txt

information infrastructure is centred around crisis management, registry and document control services, and the operation of NATO's centralised computer facilities at its headquarters.[4]

The **NATO Integrated Data Service (NIDS)** facilitates computer access to NATO documents on key issues in the fields of security and international co-operation. With the goal of contributing 'to a positive debate and to informed discussion about security issues,' NIDS is expanding by degrees its networking abilities with various Ministries of Foreign Affairs, Ministries of Defence, and parliaments in NATO and EAPC countries, in order to facilitate communication and information exchange.[5]

Assessment of Phenomena Undermining Dependability

At the conclusion of the Kosovo conflict, a Serbian state-sponsored attack on NATO's information and communication infrastructure succeeded in eliciting a denial-of-service (DOS) response form NATO's servers, however the attack did not succeed in significantly disrupting NATO information activities on a systematic level. An action such as this would be considered an Information Operation, or an action 'taken to influence decision makers in support of political and military objectives by adversely affecting adversary information and/or information systems and protecting one's own information and/or information systems.' Note that the NATO definition of Information Operations contains both defensive and offensive actions towards information systems, highlighting the dual nature of information warfare as both a security and an intelligence strategy.[6]

NATO's C3 Agency (Consultation, Command, and Control) has issued reports regarding its research into different security issues. A list of example reports and a detailed description of the NC3A can be found in Section 7. Topics covered concern encryption techniques and keys, firewalls, and the flagging of intruders and breached security. These topics can be presumed to be related to perceived threats. NC3A has since then issued a report, *Information Operations from the NC3A Perspective*, which outlines threats from the viewpoint of information warfare. This reports cites Martin Libicki's delineation of information warfare into 7 categories: Command and Control Warfare (C2W), Intelligence-based Warfare (IBW), Electronic Warfare (EW), Psychological Warfare (PSYW), Hacker Warfare (HW?), Economic Information Warfare (EIW), and Cyber-warfare. NATO's definition of Information Operation corresponds with Libicki's C2W (Command and Control Warfare). This report highlights several security concerns and security management tools:

- the proliferation of network connectivity that allows not only worldwide connectivity but also knowledge of associated protocols and applications.

- the prevalence of commercial off-the-shelf (COTS) technology in military systems has many security implications. This method of technology acquisition has both financial and operational benefits, however vulnerabilities and design weaknesses of these applications can be known on a relatively large scale. Specific security risks of COTS include 'Easter Eggs' – undocumented strings of code hidden within applications that have no relation to the intended use of the application. Easter Eggs are supposedly harmless, but demonstrate the reality of unknown, and potentially malicious, capabilities within COTS. Also, revision-tracking capabilities of some COTS word-processing applications are of concern in regards to declassified documents. Additionally, teleworking demands applications with ease-of-use and portability, an aspect

[4] NATO Handbook. www.nato.int/docu/handbook/2001/hb140806.htm

[5] www.nato.int/structur/nids/nids.htm

[6] Parker, Richard et al. *Information Operation from the NC3A Perspective*. Pg. 1. Received via personal communication.

more characteristic of COTS. Open-source applications which have been validated for robustness in the public arena may offer a solution to design problems of proprietary software such as Windows. However, one valuable aspect of COTS is that they may include hidden features which can identify source computers – a useful tool in forensics.

- Network sniffers, which passively monitor traffic on Ethernet LANs. Sniffers can supply information on TCP/IP and traffic flows, commandeer a user's session, and intercept email, account names, and passwords.

- Network mapping and discovery tools that generate maps of the network connectivity and systems. This tool can be used to locate unauthorised users and identify connectivity problems.

- Intrusion detection systems (IDS) monitor traffic and forward information to a separate analysing system. This tool looks for behaviour patterns (such as keyword or command sequences) that match known exploitation schemes.

Examples of specific exploits include:

- NTDSDOS, a method that allows the user to view all data on a Windows NT system.

- Winuke, a Windows NT denial-of-service attack.

- Back Orifice, which allows remote and unauthorised users to take over a Windows 95, 98, and NT systems.[7]

The NATO Parliamentary Assembly's Science and Technology Sub-Committee on the Proliferation of Military Technology's has issued a report entitled *Technology and Terrorism* which includes an assessment of vulnerabilities to cyber-terrorism. In addition to the use of computer technology to facilitate traditional forms of terrorism, specific threats include the use of encryption, intelligence-, and information-gathering on computer networks. Regarding the vulnerability of the physical aspect of information systems, electromagnetic pulses (EMP) emitted by High-Power Microwaves (HPM) and High Energy Radio Frequency (HERF) guns can severely damage computers and potentially destroy circuits, microprocessors, and other electronic equipment. This method of cyber-terrorism could have significant effects on banking systems, aircraft avionics, and guidance systems, medical equipment, communication centres, and emergency response services.[8]

Organisational Initiatives Aimed at Tackling Cyber-Security/Cyber-Crime or Assisting with the Development of Dependability

NC3A

- The Communications Systems Division of the C3 Agency advises NATO on the flexibility, security, and survivability of its communications systems. The Division works closely with NATO commands and agencies, national and international agencies and organisations, and industry. Within the NC3A Scientific Programme, the Division is responsible for two Scientific and Technical Packages (STP): Communications and INFOSEC Support. The Division

---

[7] *Ibid*, pg 2.

[8] Mates, Michael. *Report: Technology and Terrorism*. NATO Parliamentary Assembly, Science and Technology Committee Sub-committee on the Proliferation of Military Technology. October 2001. Available at www.naa.be/publications/comrep/2001/au-221-e.html (downloaded December 2001)

provides support to a number of other STPs, such as Training and Exercise, NATO Airborne Early Warning and Control, Electronic Warfare and Research Studies, and Air Command and Control Support.[9]

- The Information Systems Division of the C3 Agency provides scientific advice to NATO and its major military commands regarding the procurement of systems that are 'cost-effective, fully interoperable and secure.' This Division also enhances dependability by analysing the architecture of NATO information and planning for the transition from older systems. Assesses NATO's military requirements and identifies solutions to problems. The IS Division makes use of prototyping when considering the deployment of a new technology or strategy within the laboratory-like confines of the NC3A Integrated Test-bed. The Test-bed is a laboratory used to verify military requirements and the interoperability between emerging and existing systems by allowing for the refinement of the technical specifications and the identification of previously unforeseen problems.[10] NC3A will not recommend the use of an application unless it has been test-bedded first to verify its security.[11]

- NC3A also consults the Allied Command Europe on its Automated Command and Control Systems (ACCSs). ACCSs are software programmes that 'allow the efficient exploitation of the large volumes of data which are generated in crisis and conflict monitoring for military applications.' In order to enhance the security and dependability of this information, NC3A incorporates data reduction and data selection technology.[12]

- In its report *Information Operation from the NC3A Perspective*, the agency recommends the use of redundant virus checkers of different sources at both client and servers end of communication. Additionally, NC3A suggests that effective system boundaries should be built in relation to service profiles and that these boundaries should be supplied with enforcement mechanisms. Defensive information operations to be undertaken in the event of an 'incident' should be established beforehand and should cover authority, management, and privacy issues. This report also recommended the communication of security vulnerabilities to the public forum.[13]

- NC3A has established a computer vulnerability database that automatically collects information on computer vulnerability from mailing lists, news groups, vendors, and web sites.[14]

- NC3A is currently planning the establishment of a Computer Emerging Response Team (CERT)/Computer Forensics Laboratory (CFL) in conjunction with SHAPE (the NATO School).

Research and Technology Organisation (RTO)

The RTO's Information Systems Technology (IST) Panel covers the fields of Information Warfare and Assurance (such as INFOSEC, COMPUSEC, COMSEC, TRANSEC, Information Assurance and System Assurance), Information and Knowledge Management (decision-support architectures, data mining, data warehousing, information fusion, information filtering, visualisation, knowledge-

---

[9] NATO C3 Agency. www.nc3a.nato.int/pages/frameset_org.html

[10] NATO C3 Agency: Information Systems Division www.nc3a.nato.int/pages/frameset_org.html

[11] NATO C3 Agency, personal communication.

[12] NATO C3 Agency: Information Systems Division www.nc3a.nato.int/pages/frameset_org.html

[13] Parker, Richard *et al*. *Information Operation from the NC3A Perspective* 3-4. Received via personal communication.

[14] *Ibid*, 5.

based systems, and artificial intelligence), Communications and Networks (voice data and video over disadvantaged links, network management, network security, mobile communications and satellite communications), and Architecture and Enabling Technologies (software engineering technologies, computing technologies, requirements capture, modelling and simulation technologies, modelling and simulation architectures and standards, speech and natural language processing, Groupware and collaboration tools). The IST is responsible for identifying and reviewing subjects of common interest to these fields, and reviews and recommends the establishment of research and development initiatives in these fields. IST also fosters information exchange by maintaining expert networks and co-ordinating activities with other RTO panels' common activities.[15]

The IST panel convened a symposium held in Washington, DC, from 25-27 October 1999. The 28 papers presented at the symposium, entitled 'Protecting NATO Information Systems in the 21st Century', were compiled in a final technical evaluation and covered the following topics: threats and issues, information operation and analysis, system survivability, authentication, access control and privacy, and intrusion detection and response security architecture.[16]

NATO Electronic Warfare Advisory Committee (NEWAC)

NATO views electronic warfare (EW) capabilities as 'a key factor in the protection of military forces and in monitoring compliance with international agreements and [thus] essential for peacekeeping and other tasks undertaken by the Alliance.' To this end, the NATO Electronic Warfare Advisory Committee (NEWAC) was established in 1966 to support the Military Committee, the NATO Strategic Commanders, and NATO's member-nations by acting as a concerted multinational entity to promote NATO's EW capabilities. NEWAC is composed of representatives of each NATO country and of the NATO Strategic Commanders; all members are senior military officials in their national EW organisations. NEWAC's mission is to monitor the progress achieved nationally and within the Integrated Military Command Structure regarding the implementation of agreed EW actions. While called on to help develop EW command and control concepts, NEWAC is also responsible for the development of NATO's EW policy, doctrine, operations, and educational requirements. NEWAC also assists in introducing NATO's EW concepts to partner countries in the framework of Partnership for Peace. NEWAC makes no mention of specific concerns, problems, solutions, or initiatives concerning electronic warfare, an area where definitions themselves are contentious topics.[17]

NATO Parliamentary Assembly (NATO-PA)

The Parliamentary Assembly's Science and Technology Committee has issued several reports covering the major security and policy challenges confronting Allied countries in the areas of information technology and information dependability. The 1998 special report, *The Revolution in Military Affairs*, identified information technology as a key aspect of current weapons technology. Enhancements enabled by IT such as guidance, surveillance, efficiency, and effectiveness were cited as critical force-multipliers, while at the same time increasing a potential vulnerability. The report also outlined an extant 'technology gap' between the US and its European allies, in terms of

---

[15] NATO Research and Technology Organisation; IST Panel. www.rta.nato.int/ist.htm

[16] Protecting NATO Information Systems in the 21 Century, Research and Technology Organisation IST Panel. Pub # RTO-MP-027

[17] NATO Electronic Warfare Advisory Committee (NEWAC). www.nato.int/docu/handbook/2001/hb140901.htm

both capabilities and compatibilities, making it increasingly difficult to integrate truly alliance forces into a cohesive whole.[18]

A 1999 report, *Information Warfare and International Security*, further develops the NATO-PA's position on IT issues. While recognising the importance of efforts to increase information security by nations and the need to adopt measures to strengthen and protect information systems, the report goes further by identifying priorities for realising IT security. Firstly, the report recommends the objective assessment of 'real threats' by independent groups or bodies including representatives of government, industry, the scientific community, and computer security experts. The need for initiatives aimed at raising public awareness and education of computer security and protection issues was also identified as a priority. Furthermore, legislation and law enforcement are called upon to stay current with IT developments, particularly through co-operation between computer security experts and legislators as well as public-private partnerships. Finally, the report suggests that the military 'should address many questions concerning the effective role of information warfare programmes in their general policy…. [and clarify] policy about the options for deterring an attack on vital information systems and the possible us of offensive information warfare.'[19]

The Science and Technology Sub-Committee on the Proliferation of Military Technology's recent report entitled *Technology and Terrorism* includes an assessment of cyber-terrorism[20] and specific information vulnerabilities to terrorism. The report acknowledges terrorists' increasing familiarity and use of IT and predicts an increase in cyber-attack and other types of attacks on information systems by terrorist groups, particularly within two areas: '(1) terrorist use of computers as a facilitator of their activities and (2) terrorism involving computer technology as a weapon or target.' The sub-committee's recommendations for a counter-terrorism strategy include several suggestions specific to the protection of information systems:

- The adoption of national infrastructure protection policies, including the use of strong encryption, camouflage, and electronic tracking techniques.
- The inclusion of IT defence considerations by NATO.
- A human resources investment in training and educating public sector employees on issues of cyber-security.
- An increase in international legal co-operation regarding trans-national cyber-attacks, as well as an increase in Internet monitoring and intelligence sharing.

---

[18] Ibrügger, Lother. *Special Report: The Revolution in Military Affairs*. NATO Parliamentary Assembly, Science and Technology Committee. November 1998: www.naa.be/publications/comrep/1998/ar299stc-e.html (downloaded December 2001).

[19] Ehlers, Vernon J. *Information Warfare and International Security.* NATO Parliamentary Assembly, Science and Technology Committee. October 1999. Available at www.naa.be/publications/comrep/1999/as285stc-e.html (downloaded December 2001).

[20] The sub-committee report specifically defines 'cyber-terrorism' as "any act of terrorism that uses information systems or computer technology either as a weapon or a target." The report stresses that "it is important to stress the distinction between cyber-terrorism and cyber-crime, which are similar in their use of information technology but different in their motives and goals."

- Specific to electro-magnetic pulses (EMP), High-Power Microwaves (HPM) and High Energy Radio Frequency (HERF) guns, the sub-committee recommends the further development of radiation-resistant microprocessors and high-speed plasma limiters for sensitive circuits.[21]

Committee on the Challenges of Modern Society (CCMS)

The Committee on the Challenges of Modern Society (CCMS) is an organisation run under the auspices of NATO's Scientific Affairs Division. CCMS recently held the initial meeting a project entitled Vulnerability of the Interconnected Society (VIS) in Oslo, Norway on 18 June, 2001. The meeting covered security and vulnerabilities of both civilian and military nature and was attended by representatives from ministries of defence, environment, civil defence, emergency planning, and economic affairs. Topics covered organisational and crisis management approaches used to handle vulnerabilities of critical infrastructures, communication and capacity building, and the recognition of future knowledge needs. The report from this CCMS project is aimed at 'providing CCMS and the project participants with and improve decision basis for further action and co-operation in the vulnerability field.' Recommendations towards strengthening the decision basis for future actions toward reducing information vulnerabilities are scheduled for the project's fourth workshop to be held in October 2002. The report of the CCMS's VIS project is scheduled to be finalised in December 2002.[22]

Research and Development

The *Division of Scientific and Environmental Affairs* is concerned with strengthening the scientific and technological capabilities by developing ways to promote scientific and technological collaboration between scientists within Alliance countries and also scientists of Partner and Mediterranean Dialogue countries. The Division is responsible for advising the Secretary General on scientific and technological matters of interest to NATO and for implementing the decisions of the Science Committee and directing the activities of its sub-committees and advisory panels.[23]

The *NATO C3 Agency* undertakes laboratory test-bedding and field-prototyping in order to apply competently technology to improve the operational capabilities of NATO. NC3A also focuses on using 'evolutionary acquisition' to streamline the development and fielding of new systems and equipment that can be easily specified, procured, and securely implemented.[24] NC3A publishes reports and reviews concerning emerging technologies applicable to NATO, tests, and technology. Recent NC3A publications include:

- *A Review of Satellite-based Personal Communications Services (PCS) for NATO Post-2000*. (TN-747) by R. Hind. Published: March 2000[25]

- *Secure Voice and Data Over INMARSAT MINI-M Using STU-IIB Test Report*. (TN-792) by R. Hind. Published: July 2000

---

[21] Mates, Michael. *Report: Technology and Terrorism*. NATO Parliamentary Assembly, Science and Technology Committee Sub-committee on the Proliferation of Military Technology (October 2001): www.naa.be/publications/comrep/2001/au-221-e.html (downloaded December 2001).

[22] *NATO Committee on Challenges to the Modern Society*. Memo to participants of the Vulnerability of the Interconnected Society meeting – 18 June 2001, Oslo (Norway).

[23] www.nato.int/docu/handbook/2001/hb1015.htm

[24] NATO C3 Agency, www.nc3a.nato.int/pages/frameset_welcome.html

[25] NATO C3 Publications, www.nc3a.nato.int/pages/frameset_prod.html

- Assessment of Emerging Internet Technology in 2000. (TN-831) by: R. Goode; E. Harmsen; B. Hein; R. in 't Velt. Published: March 2001

A principal aim of the *Research and Technology Organisation (RTO)* is the dissemination to the NATO nations of clear, timely, and current scientific and technical information related to defence activities. Recent RTO publications dealing with aspects of information security and dependability include:

- *Massive Military Data Fusion and Visualisation* (IST-036).
- *Awareness of Emerging Wireless Technologies* (IST-035).
- *Evolutionary Software Development* (IST-034).
- *Real Time Intrusion Detection* (IST-033).
- *Robots Systems in Military Domains* (IST-032).
- *Use of Intelligent Agents in Virtual Reality* (IST-029).
- *Inforensics* (IST-024).
- *Military Communications* (IST-023).[26]

[26] NATO Research and Technology Organisation – IST Panel: www.rta.nato.int/ISTAct.htm

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD)

Overview of the OECD

The main aim of the OECD is to promote, through resolutions and recommendations, policies for growth and employment, while preserving, at the same time, economic and financial stability. In a recent OECD forum, held in Alpbach, Austria, John Dryden claimed that the OECD is a forum, a think-tank, and a resource.[1] The developments of the Information Society and the growth of electronic commerce confirm and enhance the importance of privacy-related and security issues.

In recent years, the growth and development of information and communication technologies (ICTs) has led to their wide diffusion and application, thus increasing their economic and social impact. The OECD undertakes a wide range of activities aimed at improving the understanding of how ICTs contribute to sustainable economic growth, social well-being, and their role in the shift towards knowledge-based societies. Within this framework, an essential role is, of course, the study of security and privacy issues and how to tackle different forms of cyber-crime that may undermine the dependability.

In 1968, there was the first official involvement by the OECD in the area of information technology. In that year, the *Computer Utilisation Group* (CUG) - within the Committee for Science and Policy- was formed. Main interests dealt with the quantitative and qualitative impacts of information and communication technologies on global economic growth. The foundation of the CUG represents the starting point of the OECD's active role in the investigation on the effects of information technologies and data banks on the privacy and protection of personal information collected by computer and/or network systems.

Since then, the OECD's activities in the field of information security and cyber-crime have grown, leading to a significant number of recommendations.

Of particular relevance here (in consideration of the fact that the OECD's covenant forbids it to be involved in legal activities and recommendations) is the OECD's strong concern, expressed at the time, about member-states being in the process of devising conflicting national legislations that could have hampered the international flow of data and information, therefore hampering the potential development of information-based international economics and commerce.[2]

ICT Regulatory and Legal Developments

As mentioned above, the OECD produces considerable documentation on information technology and the information society's developments. Nonetheless, the main framework is given by four core documents, which represent and guide the OECD's approach to the issue. These will be briefly discussed below.

Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data

The Guidelines, in the form of a Recommendation by the Council of the OECD, were developed by a group of government experts under the chairmanship of The Hon. Mr. Justice M.D. Kirby,

---

[1] John Dryden (OECD), *E-business and the Digital Economy- a Policy Perspective* (21 August 2001): wko.at/alpbach/bm/dok/Dryden-e.pdf (downloaded 14 November 2001)

[2] Rathmell and O'Brien, *Information Operations – An International Perspective.*

Chairman of the Australian Law Reform Commission. They were adopted and became applicable on 23 September 1980.

They were intended to help to harmonise national privacy legislation and, at the same time, prevent interruptions in international flows of data. In fact, they call for international co-operation, stating that

> Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for trans-border flows of personal data and for the protection of privacy and individual liberties are *simple and compatible* [my italic] with those of other member countries which comply with these guidelines. […][3]

These Guidelines still represent a cornerstone because they are 'technology-neutral' as they encompass privacy issues relating to data collected and managed with or without computers or other information technologies. During the 1970s, the member-countries of the OECD came together to promote the free flow of information across their borders and to prevent legal issues related to the protection of privacy from creating obstacles to the development of their economic and social relations. The privacy Guidelines were adopted to this end. They represent international consensus on general guidance concerning the collection and management of personal information. The drafters of the Guidelines foresaw that technology would develop rapidly, and the technology-neutral approach that they adopted was to accommodate future developments. They have become, through the years, a pivotal source of guidance both for businesses and governments in devising rules and norms in the privacy domain. Two issues are of particular relevance: privacy and international flow of information.

The explanatory memorandum following the actual recommendation states this point clearly:

> […] two essential basic values are involved: the protection of privacy and individual liberties and the advancement of free flows of personal data. The Guidelines attempt to balance the two values against one another; while accepting certain restrictions to free trans-border flows of personal data, they seek to reduce the need for such restrictions and thereby strengthen the notion of free information flows between countries.[4]

The importance and timeless value of the *Guidelines* are reinforced by their acknowledgement of 'privacy' as a fundamental human right. This element allows us to view the information society in the perspective of post-war global developments. The *OECD Guidelines* underline that a number of international agreements deal with the issues under discussion, e.g. the *European Convention of Human Rights* of 4 November 1950 and the *International Covenant on Civil and Political Rights* (United Nations, 19 December 1966).

The *Guidelines* also list eight basic principles concerning the protection of privacy and secure international flows of information. These are:

- The collection limitation principle
- Data quality principle (according to which data should be relevant to the purposes for which they are to be used)

---

[3] Council of the OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (23 September 1980): www.oecd.org (visited on 7 November 2001)

[4] *Ibid*.

- Purpose-specification principle (the purposes for which personal data are collected should be specified as soon as possible)

- Use-limitation principle (personal data should not be disclosed or used for purposes other that those specified)

- Security-safeguards principle (personal data should be protected)

- Openness principle (according to which there must be a policy of openness about the developments, practices, and policies with respect to personal data)

- Individual-participation principle (setting a list of rights for the individual whose personal data are involved)

- Accountability principle

Such elements all confirm the idea that the Guidelines are far from being an outdated document and that changes in technology do not diminish the consensus achieved in 1980: despite technological advances and the evolution of an electronic environment based on worldwide information and communications networks, the Guidelines are still applicable today. Over the years, the principles set forth in the Guidelines have been put to use in a large number of national and international instruments and they are still widely used both in the public and private sectors. In that context, OECD member-countries have deemed that it is not necessary to revise the Guidelines at this time. In fact, their 'technologically-neutral' nature means that they apply to all types of personal data, whether traffic data (such as date, time, or duration) or content data (for example, information contained inside an electronic message, such as personal information like name or address, information about personal preferences, or information about the kinds of transactions conducted, what was purchased at what price, etc.) At the same time, the guidelines represent the starting block for the OECD's involvement in information assurance and security activities.

Guidelines for the Security of Information Systems

The Council Recommendation C(92)188/FINAL, known as *Guidelines for the Security of Information Systems*, was adopted on 27 November 1992, and was more specifically concerned about critical infrastructures' defence.

These Guidelines provide a set of principles aimed at enhancing the security of information systems. They also call for activities in the field of public awareness, education, technological, and economic development and international co-operation. The call for international co-operation is of particular importance since it flows from the recognition of the IS's borderless nature and the possibility of suffering crimes committed in any place. The *Guidelines for Security of Information Systems* represent a pivotal element in the OECD's 'cyber-dependability'-related activities.

> The security of information systems is an international issue because information systems and the ability to use them frequently cross national boundaries. It is a problem that may be ameliorated by international co-operation. Indeed, given the disregard of information systems for geographical and jurisdictional boundaries, agreements are best promulgated and accepted on an international level.[5]

---

[5] Council of the OECD, *Guidelines for the Security of Information Systems* (27 November 1992): www.oecd.org (visited on 7 November 2001)

The question of international standards comes up frequently, as well as that of promotion of expertise and best practice in information security. Moreover, it is stressed that common rules in the allocation of risks and liabilities in case of failures of information and network systems, as well as common investigative procedures and administrative and penal sanctions against computer-related crimes are necessary.

Government institutions and international businesses can achieve these objectives by forming their decision-making on the nine principles forming the heart of the document:

- Accountability (i.e., detail the security responsibilities)
- Awareness (i.e., awareness of the procedures available for the security of information systems)
- Democracy (i.e., information security procedures need to uphold human and democratic rights)
- Ethics (i.e., assure the legitimate use of data)
- Integration (i.e., the development of a coherent and comprehensive security approach)
- Multidisciplinary principle (i.e., not to limit security to technical matters, but consider administrative, operational, commercial, and legal issues)
- Proportionality (i.e., balance between costs, levels, procedural processes, measures, and the degree of dependence of an organisation - public or private - on an information and network system)
- Reassessment (i.e., periodic reassessment to preserve effectiveness over time in countering security breaches and cyber-crimes)
- Timeliness (i.e., effectiveness over time in countering security breaches and cyber-crimes)

On the whole, the *Guidelines for the security of Information Systems* have a rather neutral, non-controversial character, describing somewhat timeless principles, independent of government policies and world events. This is also what makes them still relevant after nearly a decade. Nevertheless, following an initial revision in 1997, the OECD is presently examining these Guidelines in order to assess their continuous effectiveness in this Internet age.

Guidelines for Cryptography

These guidelines, adopted in 1997, provide a list of principles suggesting possible national and international regulations about cryptography. The most important aspect of this document has been the explicit separation between the use of cryptographic solutions for encryption purposes and its exploitation for devising digital signatures. The document has also called for the increased liberalisation of the export of cryptographic products and systems.

Overall, the main goals of this document are to encourage the use of cryptographic solutions in order to foster confidence in networks and to help ensure data security and privacy on global networks, while preserving law enforcement and tackling the problem of the potential liabilities that those organisations providing cryptographic services might face. One finding was that all

possible rules and regulations in this area should be only market-driven and that government intervention should be limited to specific circumstances.

Moreover, within such a market-driven environment, the Guidelines state as pivotal for achieving Information Security and Assurance the co-operation between the private and the public sector. In fact, among other aims, these guidelines are intended

> to promote co-operation between the public and private sectors in the development and implementation of national and international cryptography policies, methods, measures, practices and procedures.[6]

The Guidelines for Cryptography list eight principles deemed necessary to reach the stated aims:

1. Trust in cryptographic methods (i.e., cryptographic methods should be trustworthy in order to generate confidence in the use of information and communications systems)

2. Choice of cryptographic methods (i.e., users should have a right to choose any cryptographic method, subject to applicable law)

3. Market-driven development of cryptographic methods (i.e., cryptographic methods should be developed in response to the needs, demands and responsibilities of individuals, businesses, and governments)

4. Standards for cryptographic methods (i.e., technical standards, criteria, and protocols for cryptographic methods should be developed and promulgated at the national and international level.)

5. Protection of privacy and personal data (i.e., the fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic method)

6. Lawful access (i.e., national cryptographic policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible)

7. Liability (i.e., whether established by contract or legislation, the liability of individuals and entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated)

8. International co-operation (i.e., governments should co-operate to co-ordinate cryptography policies. As part of this effort, governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade)

Guidelines for Consumer Protection in the Context of Electronic Commerce

Adopted on 9 December 1999, the goal of the *Guidelines for Consumer Protection in the Context of Electronic Commerce* is to suggest a set of principles aimed at protecting consumers who are engaging on business-to-consumer activities (B2B ecommerce is not taken into account). They do not specifically address security issues. Nevertheless, they address many concerns and issues (delivery

---

[6] Council of the OECD, *Guidelines for the Cryptography Policy* (March 1997): www.oecd.org (visited on 8 November 2001)

failures, redress, dispute resolutions) that consumers consider essential if they are expected to develop trust and confidence towards online commercial activities.

According to the OECD press release of 9 December 1999,

> the overarching principle of the Guidelines is that consumers shopping on-line should enjoy transparent and effective protection that is not less than the level of protection that they have in other areas of commerce. Among other things, they stress the importance of transparency and information disclosure.[7]

The 1999 *Guidelines for Consumer Protection* were the outcome of several months of discussions, and in particular of a workshop organised in June of that year on issues relating to authentication over the Internet using cryptographic solutions such as digital signatures. On that occasion, the actors involved (government representatives and industry leaders) emphasised the need to work towards defining similar instruments for the protection of consumers from the perils of the Internet and e-commerce in general. The underlying idea is that consumers should have the same level of security and protection in whatever environment they are shopping, be it a local store or be it cyber-space.

Phenomena Undermining Dependability

The developments of the Internet (and of the IS at large) are so fast that a complete and unbreakable set of norms is inconceivable. To be aware of this, suffice it to recall the definition of 'Internet year' as suggested in the US *National Plan for Information Systems Protection* of 8 January 2000: '…a term commonly used to mean three calendar months'[8].

As has been underlined, new developments (which are unavoidable) do not mine the value of core documents like the ones outlined above, but call for the acknowledgement of these new issues and concerns that can fit in that pattern. The main issues at stake are three:

Privacy and Personally Identifiable Information (PII): One of the most dynamic technological changes occurring today involves the marriage of information technology and the study of human genetics. Scientists collaborating in the Human Genome Project are in the process of sequencing the entire human genome, that is, the sequence of some three billion pieces of information that constitute the physical make-up of a human being. Unless restrained by law, governments, employers, insurers, and others may, in some circumstances, seek access to personal data of this kind. Concerns of this type did not exist in 1980.[9] For example, regulatory frameworks' harmonisation between countries with established data protection regimes and those with different legal arrangements would seem essential when dealing with trans-national 'tele-medicine activities'. As seems clear, privacy is still pivotal and will, supposedly, become more important in the future, in relation to such developments, while PII becomes increasingly available through genetic study.

Public-Private Relations: Dependability, far from being only a concern for governments, is a grand issue for the private sector as well. Actually, data security and the fight against cyber-abuse are not only legal matters, but also questions of economic advantage. In particular, competition can be

---

[7] OECD Press Release (9 December 1999): www1.oecd.org/dsti/sti/it/consumer/prod/Press.pdf (visited on 8 November 2001)

[8] US Government, *National Plan for Information Systems Protection* (8 January 2000): 8: www.cdt.org/security/critinfra/000107national_plan.pdf (visited on 14 November 2001)

[9] Speech by Justice Michael Kirby to an international conference on privacy in Hong Kong, *Privacy Protection – In Cyberspace Should We Just Give Up?* (13 September 1999): www.ahrchk.net/solidarity/199912/v912_14.htm (visited on 8 November 2001)

severely damaged by cyber-abuse and the distrust this may cause in the public towards the developments of the IS. This is stressed in several documents, not only released by the OECD.[10]

While not underestimating the importance of governments, in the new millennium, the OECD urges stronger co-operation between public and private sector, acknowledging also the essential role the latter has in the defence of critical infrastructures:

> Critical infrastructure has been the historic domain of governments, but in today's information technology field it is inherently the province of business and government co-operation. Business and government must and do engage in close co-operation and consultation on these issues but the final decision and implementation responsibility rests with governments. […] The shift from government to industry in the sphere of information security cannot be understated.[11]

Terrorism: Finally, a major threat is represented by terrorism. While, on the one hand, new technologies and the spreading of the Internet are seen as a great opportunity, on the other hand, nations' enhanced dependence on technology has made them more vulnerable. The OECD has expressed concerns over this issue in the last few years, and fears about the possibility of non-traditional forms of terrorism, including cyber-terrorism, have been raised. In annex 1 to the quoted paper *The Changing Nature of Information Security in a Networked World*, prepared by the Ministry of Trade and Industry of Norway, this problem is stated:

> Its clear dependence on technology has made society more vulnerable, since it can now be affected by simpler means than before. […] There is also a greater use and dependence on ICT systems in the armed forces […] ICT systems have thus become weapons platforms for those trying to inflict damage on a nation, company or individual.[12]

The commitment of the OECD in the fight against terrorism can include different actions, but with reference to cyber-security, the main roles that OECD could play are (presumably) two.

First, the OECD may play a financial role, through actions of the Financial Action Task Force on Money Laundering (FATF). A plenary meeting on the financing of terrorism was held in Washington, DC, on 29-30 October 2001. On that occasion, the FATF

> […] expanded its mission beyond money laundering. It will now also focus its energy and expertise on the worldwide effort to combat terrorist financing.[13]

---

[10] For example, the German Action programme *Innovation and jobs in the Information Society of the 21st Century* affirms this relation: "In a networked world and with the enormous mountains of data that are being created and accumulating in private hands the protection of personal data is of fundamental importance. If new services are to meet with acceptance in the information society it is essential to ensure that personal data will be handled responsibly. *So ensuring efficient data protection is also an important competition factor for the suppliers* [emphasis added]": see German Federal Ministry of Economics and Technology - Federal Ministry of Education and Research, *Innovation and Jobs in the Information Society of the 21st Century* (22 September 1999): 39 - www.bmwi.de/Homepage/download/english/innovation_and_jobs.pdf (visited on 14 November 2001).

[11] Business and Industry Advisory Committee to the OECD, *The Changing Nature of Information Security in a Networked World, Proposed Outline of Work for the Review of the 1992 OECD Guidelines for Security of Information Systems*, 2nd Edition (August 2001): 2 - www1.oecd.org/dsti/sti/it/secur/ (visited on 9 November 2001)

[12] Norway Ministry of Trade and Industry, *Society's vulnerability due to its ICT-dependence* (October 2000): 23, Annex 1 to *The Changing Nature of Information Security in a Networked World*.

[13] Financial Action Task Force (FATF) news release, *FATF Cracks Down On Terrorist Financing* (31 October 2001): www1.oecd.org/fatf/pdf/PR-20011031_en.pdf (visited 9 November 2001)

This is relevant since though not explicitly mentioning cyber-attacks and cyber-crime, the statement addresses possible financing that may be available to terrorist groups through Internet-based fraud.

Secondly, there may be risk-assessments and studies, with particular attention given to dependability and vulnerabilities of national critical infrastructures.

In the aftermath of the September 2001 terrorist attacks , the concern over terrorism (in all its forms) has risen to unprecedented levels, and the OECD is likely to reinforce its engagement in this struggle.

Tackling Cyber-Security / Cyber-Crime and Research & Development

Broadly speaking, the OECD is committed to the fight against cyber-crime in two ways: on the one hand, OECD produces documentation (resolutions, recommendations, etc.), that have the aim of directing governments and businesses in their actions in this fight; on the other, OECD raises awareness (of governments, businesses, and society) through information flow and publicly-divulged statistics.

While the former has been briefly considered in the previous section, we will here summarise some of the current 'awareness-raising' activities.

The *Committee for Information, Computer, and Communications Policy* (ICCP) addresses issues arising from the 'digital economy', the developing global information infrastructure, and the evolution towards a global information society. ICCP analyses the broad policy framework underlying the *e-economy*, information infrastructure, and information society, while studying the regulations and economics of telecommunications, including the Internet, broadband and mobile, as well as convergence of the broadcasting and cable sectors with more conventional telecommunications. The ICCP committee also addresses information security and the protection of personal data, and compiles a database covering communication indicators and telecommunication tariffs, develops performance indicators, and addresses related methodological issues.[14]

The OECD *Working Party on Information Security and Privacy* (WPISP) promotes an internationally-co-ordinated approach to policy-making in security and protection of privacy and personal data in order to help build trust in the Global Information Society (GIS) and facilitate electronic commerce. The Party is also engaged in raising awareness and exchanging information among all stakeholders with the objective of developing guidance as to how to ensure privacy and security online[15].

The DSTI ([*Directorate of Science Technology and Industry*) manages databases of internationally-comparable statistics in the areas of science, technology, and industry. These statistics and indicators underpin policy-related analytical work, particularly with respect to links between technology, competitiveness, and globalisation[16].

The *Working Party on Telecommunication and Information Services Policy* (TISP) looks at telecommunications and Internet policy, promotes the exchange of experience among OECD members, and reviews developments in information infrastructure. The focus is on regulatory

---

[14] Based on the OECD Website www.oecd.org

[15] *Ibid.*

[16] *Ibid.*

reform, the convergence of telecommunication, the Internet cable television, and broadcasting networks over fixed and wireless networks.[17]

Another source is the *Future Studies Information Base*, while the OECD *Information Technology Outlook 2000* (and now the *Information Technology Outlook 2001*) describes the fast growth in the supply and demand for information technology goods and services and their role in the expanding Internet economy.[18]

Finally, OECD provides an anti-corruption ring homepage (AnCorR) with a considerable number of selected readings.[19] The home page 'Anti-corruption ring on-line' refers to electronic crime (*e-crime*). The fast development of communications technology in the last decades has created opportunities to commit traditional types of crime, such as corruption and money laundering, in non-traditional ways. Due to the lack of sufficient national and international control mechanisms, computers and other new communication and payment techniques are among the favourite tools to conceal proceeds of fraud. This section of AnCorR provides instant access to resources assessing the impact of e-crime on corruption and money laundering and providing examples of best practices to control and prevent such crimes.

Whilst the previous activities address specifically information security themes, the OECD is also engaged in other projects, such as the *Futures Project on Emerging Systemic Risks,*[20] which is relevant for the issues under discussion. In fact, this project (2000-2002) is being conducted within the framework of the OECD *International Futures Programme* with the purpose of providing OECD governments, major players in the business sector, as well as civil society, with a common assessment of the means needed to ensure that risk management can contribute fully to the sound and sustainable evolution of the OECD area and the world economy at large. Telecommunications are - of course - part of the activity, since they represent an area at high-risk for which a bad event could cause serious disruptions both at a national and/or a global level.

Lastly, the OECD is also engaged in research and development activities, and a consistent quota of its budget is devoted to this. In fact, this expenditure has also been subject to criticisms, due to its consistent weight. In an *Inter Press Service* (IPS) article of July 2001 on the UNDP 2001 Human Development Report, Diego Cevallos reports that

> According to the UNDP document, the market is not proving - at least in the case of technology - to be making a clear contribution to the development of poor countries or attending to their needs. […] In 1998, the Organisation of Economic Co-operation and Development (OECD), a group of the 29 richest countries, spent 520 billion dollars on research and development, a sum surpassing the combined gross domestic product (GDP) of the world's poorest 88 countries, according to the UNDP.[21]

Bibliography

Council of the OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 23 September 1980

---

[17] *Ibid*.

[18] Dr Andrea K. Riener, Andrea K., *An Inventory of Preventive Multilateral Activities in the Fields of Computer-related Crime and Cyber-Threats in Europe*, Study prepared for the Forschungsstelle für Sicherheitspolitik und Konfliktanalyse an der ETH-Zürich, Vienna (July 2001): 74: www.isn.ethz.ch/crn/intorg/cyberthreads.pdf (visited 12 November 2001)

[19] *Ibid*.

[20] OECD, *OECD Futures Project on Emerging Systemic Risks* (2000-2002), *A Policy-Oriented Analysis of their Economic Significance and Prospects*: www1.oecd.org/sge/au/risks.htm (visited 12 November 2001)

[21] Diego Cevalles, Diego, "DEVELOPMENT: Technology and the Market, an Exclusive Relationship", Internet Press Service- World News (July 2001): www.undp.org/hdr2001/clips/IPStechnology.pdf (visited 12 November 2001)

Council of the OECD, *Guidelines for the Security of Information Systems*, 27 November 1992

Council of the OECD, *Guidelines for the Cryptography Policy*, March 1997

US Government, *National Plan for Information Systems Protection* , 8 January, 2000, p. 8 ff.

Justice Michael Kirby, *Privacy Protection – In Cyberspace Should We Just Give Up?*, Speech to an international conference on privacy, Hong Kong 13 September 1999

German Federal Ministry of Economics and Technology, Federal Ministry of Education and Research, *Innovation and Jobs in the Information Society of the 21st Century*, 22 September 1999, p.39 ff.

Business and Industry Advisory Committee to the OECD, *The Changing Nature of Information Security in a Networked World, Proposed Outline of Work for the Review of the 1992 OECD Guidelines for Security of Information Systems*, 2nd Edition, August 2001, p.2 ff.

Norway Ministry of Trade and Industry, *Society's vulnerability due to its ICT-dependence*, October 2000, p. 23 ff., Annex 1 to The Changing Nature of Information Security in a Networked World.

FATF news release, *FATF Cracks Down On Terrorist Financing*, 31 October 2001

Andrea K. Riener, *An inventory of Preventive Multilateral Activities in the Fields of Computer-related Crime and Cyber-Threats in Europe*, study prepared for the Forschungsstelle für Sicherheitspolitik und Konfliktanalyse an der ETH-Zürich, Vienna, July 2001, pp. 74-75

OECD, *OECD Futures Project on Emerging Systemic Risks (2000-2002). A Policy-Oriented Analysis of their Economic Significance and Prospects*

Diego Cevalles, *DEVELOPMENT: Technology and the Market, an Exclusive Relationship*, Internet Press Service- World News, July 2001

Abbreviations

AnCorR	Anti-Corruption Ring homepage
CUG	Computer Utilisation Group
DSTI	Directory of Science Technology and Industry
FATF	Financial Action Task Force
GDP	Gross Domestic Product
GIS	Global Information Society
ICCP	Information, Computer and Communications Policy
ICT	Information and Communication Technologies
OECD	Organisation for Economic Co-operation and Development
PII	Personally Identifiable Information
TISP	Telecommunication and Information Services Policy
UNDP	United Nations Development Programme
WPISP	Working Party on Information Security and Privacy

UNITED NATIONS (UN)

Overview

The formal involvement of the United Nations in the Information Assurance field is very recent; although activities related to Information Security and computer crime have been discussed by many UN-related organisations since the end of the 1980s, the main bases of the United Nations' position on all issues dealing with information – and therefore information security – are Articles 19 and 27 of the Universal Declaration of Human Rights, which defines free access to information as one of the basic human rights. Also due to its mission of reducing poverty, the UN is concerned with the use of technology for social and economic development. Notwithstanding the multiplicity of activities, this UN involvement presents some general traits. In light of its global membership, the UN has aimed at devising a general set of norms and rules matching the global span of the Internet which also reflect the economic and social particularities of its member-states. This approach can be seen in both the deliberations of the UN General-Assembly, as well as the many UN specialised agencies. Although assessing the individual effectiveness of these efforts can be quite complex, it is worth noting that these activities have had the invaluable role of fostering debates regarding the employment and diffusion of the Internet and its associated information and network technologies, as well as educating and raising awareness regarding associated risks and threats. These have confirmed, in particular, the importance of constant dialogue between state institutions and international businesses to devise information exchanges regarding security breaches.

The General-Assembly of the UN does encounter issues related to ICT. The UN also has several specialised bodies that deal more closely with issues surrounding ICT:

1. Within *UNESCO* (United Nations Educational, Scientific and Cultural Organisation), information and security issues fall within the General Information Programme (PGI) and the Intergovernmental Informatics Programme (IIP) of Major Programme IV.

    a. *PGI* covers development issues as they relate to 'Informatics and Infostructure' such as access to information, privacy, confidentiality, security of information, observing the national policies and legal frameworks surrounding these issues. Most of the policies and initiatives of PGI are directed towards the South, notable exceptions being the 1999 Workshop on Information Strategies in the 21st century[1] and the recently commissioned UNESCO/FID study on national information policies and strategies.[2]

    b. The *IIP* focuses on developing human resources through knowledge sharing.[3] Most notably, the IIP is responsible for the *Information Society Observatory*, which monitors the 'Ethical, legal and societal challenges of the Information Society' by acting as a clearing hose for information on action plans and policies of countries and organisations.[4] UNESCO also sponsors the *Free Software Portal*, which disseminates free software licences and developer software.[5]

---

[1] UNESCO WebWorld: www.unesco.org/webworld/public_doman/index.html

[2] Study on National Information Policies: www.unesco.org/webworld/highlights/fid_220299.html

[3] www.unesco.org/webworld/iip/index.html#objectives

[4] Information Society Observatory: www.unesco.org/webworld/observatory/index.shtml

[5] Free Software Portal: www.unesco.org/webworld/portal_freesoft/index.shtml

2. Also present is the United Nations Commission on International Trade Law (*UNCITRAL*). This body is responsible for the Model Law on Electronic Commerce and the *Model Law On Electronic Signatures.*

3. Most recent was the launching of the *UN ICT Task Force*, whose formation was recommended by the Economic and Social Council to the Secretary-General.

Analysis of the Main Regulatory and Legal Developments Related to Information and Telecommunication Systems and Services

Examples of recent and projected legislative measures aimed at enhancing information and telecommunication services include UNCITRAL's *Model Law on Electronic Commerce* and *Model Law On Electronic Signatures* (see below). Various initiatives for expanding access to the Internet and other information infrastructures and services include those by UNESCO, which has maintained efforts to increase the means available to developing countries for the production and distribution of information and programmes. The focus is not only ICT but also press, radio, television, and news agencies.[6] The 30th session of UNESCO urged all member-states to promote the free and universal access to public domain information. UNESCO has many initiatives aimed at expanding access to ICT, the majority of which are aimed at the South. There is also the UN Development Programme's (UNDP) Digital Opportunity Initiative, which is aimed at increasing ICT infrastructures in the underdeveloped countries.

E-Government initiatives: While the focus of the UN is more on the upstream access of technology, the organisation does implicitly and explicitly support the downstream availability of e-government to citizens. For example, UNESCO's most recent InfoEthics conference held governmental information availability as one of the sub-themes of the gathering. In the Final Report of the InfoEthics 2000 conference, member-states were advised to make governmental information and services available online as well as developing a dialogue with citizens and NGOs.[7]

Government-led initiatives aimed at fostering electronic commerce: UNCITRAL's *Model Law on Electronic Commerce* addresses general norms rules for electronic commerce in specific areas, such as carriage of goods.

General legal principles and developments related to the ICT environment; overview of relevant new legislation: The Declaration of Sana'a (1996) instructs Arab governments to work with the UN and UNESCO, other governmental and non-governmental bodies, and most notably to enact or revise laws in order to make free access to information legally enforceable.[8]

In January 1999, the General Assembly adopted the resolution *Developments in the Field of Information and Telecommunications in the Context of International Security*,[9] following the introduction of the text by Ambassador Vasily Sidorov, Representative of the Russian Federation to the UN, on 14 October 1998. The objective was to stir debate and action inside the UN in this domain in light of the potential international security impact of the Internet. In introducing the text of the draft, Ambassador Sidorov emphasized that the proposal was not intended to be confrontational, but rather "strives for consensus and searches for ways to solve the problem through collective wisdom, joint efforts and on the basis of a common interest on the part of the international

---

[6] *Medium-term strategy for 1996-2001*, Adopted by the General Conference at its 28th Session, 1995

[7] *Final Report*, InfoEthics 2000: webworld.unesco.org/infoethics2000

[8] *Declaration of Sana'a*, 11 January 1996. Resolution 34 of the 29th Session of the General conference of UNESCO, 1997.

[9] UN General Assembly Resolution 53/70 Document A/Res/53/70 (4 January 1999)

community".[10] The final text of the resolution partially reflected the objectives of the Russian Federation, a clear statement that Russia would like to see some form of international legal regulation of the worldwide development and malicious use of information technology, in the same way as development and export of missile technology has been regulated and guided by the MTCR. More obvious parallels can be drawn between the various Nuclear, Chemical, and Biological agreements and treaties, designed not only to prevent use but to ensure that arms races are controlled. Many military thinkers in Russia argue that the effects of Information Warfare could potentially be just as bad as those of a nuclear detonation (i.e., widespread destruction of a nation's critical life-support infrastructures). Therefore, treaties similar to SALT, ABM, and START are required to govern the development of IW capabilities, as well as use.[11] The resolution reacts to this threat by inviting member-states to promote dialogue around information technology and security issues such as information warfare. Additionally, the resolution calls for a consideration of the possible development of "international principles that would enhance the security of global information and telecommunication systems and help combat information terrorism and criminality."[12]

After this adoption, Information Security and Assurance were the topics of a workshop organised by the United Nations Institute for Disarmament Research in Geneva in July 1999.[13] Experts from many UN member-states detailed the complexities related to achieving Information Security and Assurance in a global digital environment. In particular, delegates discussed issues related to the RMA, as well as the proliferation of offensive tools to breach the weak defences of information and network systems. At the end of the programme, delegates confirmed the vulnerability of National and International Information Infrastructures to cyber-attacks. There was, therefore, a strong need to improve Information Assurance. In light of the Internet's global nature, states were called on to structure a global dialogue in devising trustworthy systems and protecting information infrastructures. The General-Assembly of the United Nations was highlighted as an appropriate forum in which solutions could be devised and awareness raised.

The delegates also considered the potential international legal implications of Information Assurance and Information Warfare. There were questions concerning the possibility of undertaking Information Operations as part of UN-mandated sanctions and enforcement operations. Delegates also debated potential measures to control the proliferation of offensive Information Warfare capabilities and the possible adaptation of the existing Laws of Armed Conflict to the Internet arena. The workshop also looked at possible defensive Information Warfare approaches, calling on UN member-states to devise measures for developing trustworthy systems using the present new technologies, standards and norms while, at the same time, respecting civil liberties and cultural differences. The main conclusion of the workshop was that the protection of information infrastructures was not only a military or strategic issue but mainly a social responsibility.

---

[10] Permanent Mission of the Russian Federation to the United Nations, "Statement by Ambassador Vasily Sidorov, Representative of the Russia Federation in the First Committee of the 53rd Session of the UN General Assembly, October 14th, 1998": www.un.int/russia/statemnt/ga/53rd/1st_com/98_10_14.htm (downloaded 27 July 2000).

[11] Responses to Resolution 53/70 ("Developments in the Field of Information and Telecommunications in the Context of International Security") by the Permanent Mission of the Russian Federation to the United Nations in New York (9 June 1999).

[12] *Developments in the Field of Information and Telecommunication in the Context of International Security*; Responses to Resolution 53/70 (9 June 1999).

[13] UNIDIR, "Development in the Field of Information and Telecommunications in the Context of International Security-Private Discussion Meeting Hosted by DDA and UNIDIR, August 25-26 1999": www.unog.ch/UNIDIR/eiw.htm (downloaded 1 August 2000).

The 54th General-Assembly of the United Nations in September 1999 again saw Russia as the main proponent of information security.[14] In presenting the resolution, a senior Russian diplomat emphasised the need to work towards a multilateral declaration first, and eventually towards an international treaty indicating commonly accepted principles of Information Security. He proposed that this document would create the necessary conditions for a safe and equal international exchange of information to prevent the use of information technologies for terrorist and criminal purposes and, more importantly, information wars.[15]

Unlike the previous year, however, there were strong criticisms of this resolution. In November 1999, it was concluded that "this resolution has not yet worked out what its is wanting to do, beyond waving a coded flag of warning about the implications of US technology dominance, the so-called Revolution in Military Affairs (RMA) and the potential for information and high tech warfare". Member-states were encouraged to inform the Secretary-General about their opinions surrounding Information Security definitions and the possibility for international principles, while suggesting possible measures to combat cyber-terrorism and crime.[16] In the 2000 UNGA debates on the Russian proposal, the resolution continued to be considered under First Committee deliberations, despite moves by the US, UK, France, Germany, and others to push the debate elsewhere within the UNGA committee system. Resolution 54/50 stated that science and technology should be available to be used 'to safeguard international security and that international co-operation in the used of science and technology through the transfer and exchange of technological know-how for peaceful purposes should be promoted' and the 'Member States to undertake additional efforts to apply science and technology for disarmament-related purposed and to make disarmament-related technologies available to interested States.'[17]

Assessment of Phenomena Undermining Dependability

Access: the UN as a whole focuses on issues of access to ICT. Such access is seen as being intrinsic to economic and social development, equality, and education.

Copyright and Intellectual Property Rights: piracy and counterfeiting of copyrighted material is cited as costing tens of billions of dollars every year. However, UNESCO recognises that copyright laws can be counter to the establishment of a 'robust public domain' and advises member -states to maintain this principle within their copyright laws.[18]

Fraud: the concern for this criminal activity is implicit in the formation of the UNCITRAL's Model Laws on Electronic Signatures and Electronic Commerce.

Organised Crime: UN Convention Against Transnational Organised Crime was in part precipitated by the opportunities for crime opened up by communication technologies (see below).

Organisational Initiatives Aimed at Tackling Cyber-Security/Cyber-Crime or Assisting with the Development of Dependability

United Nations Educational, Scientific, and Cultural Organisation (UNESCO): UNESCO's involvement in Information Security and Assurance derives from its activities concerning the

---

[14] UN General Assembly Resolution 54/49 Document A/Res/54/49 (23 December 1999)

[15] Rathmell and O'Brien, "United Nations", *Information Operations: An International Perspective*.

[16] *Ibid*.

[17] Resolution 54/50 to the 54th Session of the United Nation's General Assembly (23 December 1999)

[18] *Final Report*, InfoEthics 2000: webworld.unesco.org/infoethics2000

Internet's impact on the spread of child pornography, paedophilia, and privacy violation. The objective of this organisation is to find a balance between the protection of an individual's dignity and rights through Information Security technologies, with services such as cryptography, and their malicious use by criminals or paedophiles. UNESCO believes that this balance is essential for creating a positive perception of trust and trustworthiness towards digital technologies and services. In order to accomplish these objectives, UNESCO has launched, following a meeting that attracted over 300 experts from all around the world, an action plan aimed primarily at curbing sexual abuse, child pornography, and paedophilia over the Internet.[19]

The first objective of the programme is to foster research activities to obtain a comprehensive and more up-to-date understanding of these issues. Moreover, UNESCO wants to facilitate the exchange of information among researchers to devise common solutions that reflect local cultural heritages and mores. Several solutions have been indicated, such as a network of national hotlines where children and other victims may get the necessary assistance, or the establishment of a world network of strategic citizens and personalities, institutions, and industry against these terrible activities. Nevertheless, UNESCO believes that its most important role is to assist in the creation of an international legal framework to counter these crimes. Similar to the objectives of the G8 and ODCCJP, UNESCO wants to eliminate "data havens" where criminals may freely carry out their operations.

UNESCO believes that this framework must be built from a combination of three principles. First, there is a need for targeted regulation such as anti-child pornography laws covering possession of images or other digital material. The second principle refers to self-regulation, mainly directed at industry which is expected to develop codes-of-conduct for assisting law enforcement. In particular, UNESCO has targeted the role of ISPs in 'supporting' paedophiles through use of their networks. Finally, UNESCO strongly supports co-regulation where all the stakeholders (governments, industry, and citizens) come together to devise international norms and regulations. Specifically, UNESCO wants to see a frank dialogue balancing government and ISP interests in terms of monitoring data traffic and related business and legal issues.

The 29th session of the General Conference of UNESCO in 1997 stated as a goal 'to help Member States formulate national and regional policies for the development of information technologies, while promoting access to the Internet as a public service and telematics applications for development, and provide support for regional programmes of specialised information.' This session also supported the establishment within UNESCO of an international instrument on the establishment of a legal framework relating to cyber-space and instructed the preparation of regional and international expert meetings to ascertain policy priorities and needs of member-states and to report back at the 30th session.[20] The resulting report of the Experts Meeting on Cyber-space Law laid out several principles for the Director-General of UNESCO. Of note are the Universal Service Principle, Ethics Principle (urging efforts to develop ethical guidelines for participation in cyber-space), Privacy and Encryption Principles (which support the right to privacy and secrecy of communication and urges the use of technical and legal remedies to privacy issues), and the International Co-operation Principle (which urges states to "co-operate at an international level and to harmonise national laws to resolve jurisdictional or conflict of laws differences"). This report also recommended several actions to be undertaken by the UN, such as a study of the application to cyber-space for each article of the Universal Declaration of Human Rights, to

> 'conduct an independent study of the actual economic cost of piracy on the Internet and degree to which the resulting disincentive has reduced the supply of works desired by the

---

[19] UNESCO, "Sexual Abuse of children, Child Pornography and Paedophilia on the Internet: An International Challenge", Expert Meeting, UNESCO, Paris (18-19 January 1999): www.unesco.org/webworld/child_screen/conf_index.html (downloaded 21 May 2000).

[20] The 29th Session of the General Conference of UNESCO. Paris (21 October to 12 November 1997): 58.

public', and to 'study the significance of jurisdictional issues and conflicts of law and promote harmonisation of national laws'.[21]

UNESCO echoed these sentiments in 2000 by advocating legislative and organisational harmonisation between member-states, but also by supporting the "development of legal frameworks, which include freedom of information and protected disclosure laws".[22]

United Nations Economic Commission for Europe (UNECE): Notwithstanding its role in monitoring European economic development, UNECE has been heavily involved in activities related to Information Assurance and Security since the end of the 1980s. In 1987, UNECE released the *UN Electronic Data Interchange for Administration, Commerce and Transport Standard* (UN/EDIFACT). The objective of this initiative was to devise a single international standard for the exchange of data over EDI to improve efficiency in administrative and trade procedures. In 1995, UNECE continued its strive towards harmonisation for EDI exchanges through the release of a "Model Interexchange Agreement for the International Commercial Use of Electronic Data Interchange". The security of messages and data was one of the pivotal elements of this initiative.[23]

In 1996, UNECE began to support the promotion and harmonisation of digital exchanges of data and information. Senior managers had come to the conclusion that the Internet and its associated services and technologies required detailed attention if governments and industry wanted to collect economic and social rewards. The end result was the establishment of the *United Nations Centre for Facilitation of Procedures and Practices for Administration, Commerce and Transport* (UN/CEFACT). Its objectives are:

- to analyse the key activities and elements of international transactions
- to identify the procedural constraints that affect them, including requests for unnecessary or duplicate information, and
- to develop recommendations to eliminate identified constrains, simplify data flows, and harmonise remaining procedures.[24]

One of the first UN/CEFACT activities was to release, in 1999, an updated draft for electronic transactions. Unlike the previous attempt, the present one is technologically-neutral because of the dynamic Internet environment. Still, similar to the previous one, specific attention has been devoted to data and information security of e-transactions, especially in relation to issues such as the liability of a provider of the telecommunication services. [25]

United Nations Conference on Trade and Development (UNCTAD): The mandate of this UN organisation is to maximise trade, investment and commercial opportunities for developing countries. Due to the growing cost-efficiency provided by information and telecommunication services, the Internet and e-commerce are perceived as important elements in accomplishing these

---

[21] *Report to the Director General by the Experts meeting on Cyberspace Law.* Monaco, 29-30 September 1998.

[22] *Final Report*, InfoEthics 2000. webworld.unesco.org/infoethics2000

[23] Information collected from UN/ECE "The Commercial Use of Interchange Agreements for Electronic Data Interchange", Recommendation 26 adopted by the Working Party on Facilitation of International Trade Procedures, Geneva (March 1995) Doc. TRADE/WP.4/R1133/Rev.1: www.unece.org/cefact/rec/rec26en.htm (downloaded 29 May 2000).

[24] "Knowledge of UN/CEFACT": www.uncece.org/cefact/knolwlg/knowlg.htm (downloaded 29 May 2000).

[25] UNECE/UNCEFACT, "Electronic Commerce Agreement": www.onnet.se/lwg/w4w1.htm (downloaded 29 May 2000).

objectives in the near future. Nevertheless, these goals can only be reached through an international commercial code for electronic commerce. In particular, UNCTAD has emphasised the urgent requirement to "establish the legal validity of electronic documents and the acceptability of digital signatures and other authentication procedures used in commercial transactions". In this context, UNCTAD considers Information Security and e-commerce authentication services as pivotal instruments.

In 1992, UNCTAD launched the Trade Efficiency Initiative (TEI) to assist small- and medium-enterprises (SMEs) from developing countries in deriving benefits from information and network technologies. The TEI was based on the premise that developing countries do not have the technical and human resource-capabilities to operate in a digital environment. Moreover, local universities and advanced education centres do not have the knowledge to devise courses or specialisations in this area. As part of TEI, UNCTAD launched the Trading Point Programme that provides electronic trade facilitation centres and training initiatives through TRADEFORTRADE/ETRADE courses. Presently, there are more than 100 centres around the world; interestingly, some of these are operated by technology-based companies providing services such as web-hosting. These Trade Points also offer supporting services for electronic authentication and digital signatures. This initiative has been structured as part of the SEAL (Security Electronic Authentication Link) programme that focuses on developing public key infrastructures for e-commerce based on the use of smart-card technologies.[26]

United Nations Institute for Disarmament Research (UNIDIR): Following the adoption of Resolution 53/70, UNIDIR held a workshop concerning Information Security and Assurance.[27] The workshop hosted experts in information security as well as delegates from member-states. Topics considered covered possible breeches of information security and the legal implications of sanctions and enforcement operations concerning information warfare and security. States were called upon to respect civil liberties and cultural differences while devising systems to address the vulnerability of information systems.[28]

United Nations Centre for International Crime Prevention-Office for Drug Control and Crime Prevention: Every five years, the UN organises international congresses on the prevention of crime and treatment of offenders. These meetings provide the setting for in-depth discussions concerning new norms for curbing organised crime, as well as fostering international co-operation, in order to pave "the way for more human and effective methods of crime management". One of the pivotal elements of these congresses is information-sharing among national law enforcement communities that eventually allows for the renewal and upgrading of existing systems and practices, as well as the development of international guidelines.

The fight against computer crime and – indirectly – offensive Information Warfare, has been a topic of debates and actions since the Eighth Congress held in Havana in 1990. On that occasion, participants agreed on the need to modernise national criminal laws to provide the law enforcement community with the necessary instruments to tackle these issues. There was a call, in particular, for devising new offences, as well as investigative and evidentiary procedures, to deal with these new activities. Similar discussions were carried out during the following Congress in Cairo in 1995. At a time, however, the global success of the Internet and its associated information and network technologies, beyond the closed settings of government and international businesses,

---

[26] Information collected from "Implications for Trade and Development of Recent Proposals to Set Up A Global Framework for Electronic Commerce: A Report by the UNCTAD Secretariat", UNCTAD Doc. TD/B/Com.3/17 (22 September 1998).

[27] *Development in the Field of Information an Telecommunication in the Context of International Security-Private Discussion Meeting Hosted by DDA and UNIDIR.* UNIDIR (24-25 August 1999): www.unog.ch/UNIDIR/eiw.htm

[28] Rathmell and O'Brien, "United Nations", *Information Operations: An International Perspective*.

was still very much in its infancy. The environment was completely different in April 2000 when Vienna hosted the Tenth Congress.

Delegates were now faced with an increasingly interconnected world. Strong international co-operation to fight computer crime was now vital. However, delegates appreciated the need to devise global norms and rules that match the Internet and its open and flexible architecture. The complexities and difficulties of this issue were discussed during a Workshop on Crime related to Computer Networks. This workshop was initially endorsed by two General-Assembly resolutions (in December 1998 and December 1999) calling for the Tenth Congress to organise a technical meeting for dealing with issues related to crime carried out or enhanced by the Internet and its associated technologies. [29]

The *Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders* carried out most of the preparatory work for this workshop by organising several expert meetings that resulted in a final report. Raising public awareness towards computer crime issues was indicated as a priority, in conjunction with the need to move toward a common international policy. New investigative measures and cross-border co-ordination and assistance were also mentioned. In particular, states were invited to create national contact points, similar to those created among G8 members, to advise requesting countries about the assistance that could be given in order to initiate the measures for the investigation and prosecution of cyber-criminals.

Following lengthy discussions, the Tenth Congress concluded that computer-related offences should be criminalised and that, therefore, there was a need for adequate laws regarding the investigation and prosecution of cyber-criminals. Further actions with regard to the provision of technical co-operation and assistance concerning crime related to computer networks were also invited. The most interesting conclusion referred to the need for strong state-business co-operation. Delegates tackled the complexities of how to combine the interests of the law enforcement and business communities, in particular in the areas of evidence gathering. As indicated in the concluding statement, delegates agreed that:

> when evidence sought by law enforcement was in the computer systems of a legitimate business, the search might cause harm to the business if it interfered with computer operations. It was agreed that, in such cases, the challenge was to execute the search effectively but without disrupting normal business operations.[30]

The UN Convention Against Transnational Organised Crime was in part precipitated by the opportunities for crime opened up by communication technologies. The convention encouraged Member States to support each other with resources and technical expertise. Article 18 of the Convention allows for the use of electronic media to speed up the process of the collection of evidence 'where the governments involved are satisfied as to measures taken regarding such things as authenticity, security and confidentiality.' The article also explicitly supports the use of video - conference for the taking of evidence from witnesses. There is no mention of allowances for digital surveillance in this convention.[31]

United Nations Information & Communications Technologies Task Force: the *UN ICT Task Force*, launched on 20 November 2001, is mandated to "provide overall leadership to the UN role in helping to formulate strategies for the development of information and communication

---

[29] United Nations, "Crimes Related to Computer Networks: Background Paper for the Workshop on Crimes Related to Computer Network", Doc. A/CONF. 187/10 (released 3 February 2000).

[30] "Report of Committee II-Workshop on Crimes Related to the Computer Networks", 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders, UN Doc. A/CONF 187/l.10 (16 April 2000).

[31] *UN Convention Against Transnational Organised Crime* (12-15 December 2000): www.odccp.org/palermo/convmain.html

technologies and putting those technologies at the service of development". Task Force priorities are defined by the ECOSOC 2000 Ministerial Declaration as:

1. To forge strategic partnerships between the United Nations system, private industry, trusts and foundations, donor governments, programme countries, and other relevant international actors.

2. To pool the experiences of both developed and developing countries in introducing and promoting ICT for development.

3. To develop innovative modalities for strengthening the ICT capacity of the developing countries.

4. To assist member -states in the creation of national ICT strategies, policy frameworks, and regulatory environments to ensure connectivity and universal access to ICT.

5. To promote ICT for development applications: building human resources and institutional capacity, including e-health, e-education, e-government, and e-commerce.

6. To mobilise new and additional resources - financial, technical, and human - for promoting and funding ICT-for-development programmes and projects.

The aim of the Task Force is to facilitate and support existing and planned initiatives of other bodies; the Task Force "will not develop operational or implementing capacity".[32] The members of the Task Force come from the public and private sectors, from civil society and the scientific community, and from leaders of the developing as well as the most technologically-advanced countries The Task Force is mandated by UN Secretary-General Kofi Annan to find new, creative and quick-acting means to "spread the benefits of the digital revolution – from which four billion of the world's people are currently excluded". Proposed Working Groups for the ICT Task Force include ICT Policy and Governance, National and Regional e-Strategies, ICT Business and development applications, Resource Mobilisation, Connectivity and Access, and Enterprise and Entrepreneurship.

Government schemes aimed at fostering the use of dependability-enhancing technologies and services: The United Nations Commission on International Trade Law (UNCITRAL) has developed a *Model Law On Electronic Signatures*. Since its establishment in 1966, UNCITRAL has been the core legal body of the United Nations system in the field of international trade law, as well as the main vehicle for the removal of potential barriers for the free international flow of goods and services. UNCITRAL's initial involvement in electronic commerce began when the use of the Internet and its associated information and network technologies were still restricted to military or educational environments. International businesses were developing so-called electronic data interchanges (EDIs) based on leased data lines and proprietary communication and transmission protocols. In 1985, UNCITRAL released a recommendation inviting national governments to review their legal and commercial rules concerning computer records. Particular attention was paid to their use as evidence in litigation, as well as the possible substitution of handwritten signatures with digital ones for specific electronic trade and transactions. The UN General-Assembly later approved the recommendation and called for actions for assuring security in the context of the widest possible use of automated data processing in international trade.[33]

---

[32] UN ICT Task Force: www.unicttaskforce.org

[33] "Resolution on the Legal Value of Computer Records", United Nations Commission on International Trade Law Yearbook, Part One, Section D, vol. XVI (1985): www.un.or.at/uncitral.

In their report to the General-Assembly, the Working Group on Electronic Commerce issued a *Draft Guide to the Enactment of the UNCITRAL Model Law On Electronic Signatures*.[34] This Working Group "expressed overall satisfaction with the structure and contents of the draft Guide to Enactment". Many recommendations towards changes were focused on phraseology and calls for the further elaboration of statements. The *Model Law On Electronic Signatures* is intended to have a significant role in enhancing the use of paperless communication and is based on the establishment of a functional electronic equivalent for paper-based concepts such as "writing", "signature", and "original".[35]

Following the *Model Law on Electronic Commerce*, in 1997 UNCITRAL decided to focus on drafting uniform rules for digital signatures.[36] After several discussions among government and industry experts, the Commission decided to move temporarily away from the principles of technology neutrality and media neutrality by focusing on asymmetric or public key cryptography. They rightly believed that it would have been extremely difficult to address the legal effects of various types of electronic signature techniques. These proposed rules focused primarily on the obligations of the holder of the digital signature, as well as the obligations of those organisations that provide and manage the digital certificate.

The *Model Law on Electronic Commerce* has already affected the legislation of a few countries and currently a survey is being done on the case law, court, and arbitral decisions interpreting national legislations that have been constructed around the Model Law.[37] With a view to assisting executive branches of Governments, legislative bodies, and courts in enacting and interpreting the Model Law, the Commission has produced a *Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce*.[38]

In January 2002, the UN announced the formation of a World Summit on the Information Society to "address the digital divide" in order to "harness the development potential of ICT".[39] The Summit, which is expected to promote access by all countries to information, knowledge, and communications technologies for development, is to be held in two phases, the first in Geneva in 2003 and the second in Tunisia in 2005 and is being convened under the high patronage of the UN Secretary-General, Kofi Annan. The International Telecommunication Union (ITU) will be taking the lead role in the Summit preparations, in co-operation with other interested organisations and partners. Resolution A/RES/56/183 calls on governments to participate actively in Summit preparations and to be represented at the highest possible level. The resolution has also asked for the active participation and effective contribution in the Summit and its preparations by all relevant United Nations and intergovernmental organisations, including international and regional institutions, as well as non-governmental organisations, the civil society, and the private sector. The ITU will work to create synergies and develop co-operation among the various ICT initiatives at the regional and global level.

The World Summit on the Information Society is an initiative of the 1998 Plenipotentiary Conference of ITU and endorsed by the General-Assembly as an effective means to assist the United Nations in fulfilling the goals of the Millennium Declaration - the landmark document

---

[34] *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment* (Adopted 1996): www.unicitral.org/english/texts/electcom

[35] *Report of the Working Group on Electronic Commerce on its 38th Session*. Document A/CN.9/484 (24 April 2001).

[36] UNCITRAL, "Planning Of Future Work On Electronic Commerce: Digital Signatures, Certification Authorities, And Related Legal Issues", Doc. A/CN.9/WG.IV/WP.71 (31 December 1996): www.un.or.at/uncitral.

[37] *Ibid*, 25.

[38] *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment* (Adopted 1996): www.uncitral.org/en-index.htm

[39] ITU Press Release (9 January 2002): www.itu.int/newsroom/press_releases/2002/UNGA_res_56_183.html

adopted by a record number of leaders when they met during the Millennium Summit to address the key challenges of our time. Secretary-General Kofi Annan states, "the Millennium Summit recognised the key role of partnerships involving governments, bilateral and multilateral development agencies, the private sector and other stakeholders in putting ICTs in the service of development." The General-Assembly has also invited the international community to make voluntary contributions to a special trust fund established by the ITU to support the Summit, as well as to facilitate the effective participation of representatives of developing countries, in particular those from the least developed countries.

The proposed themes of the Summit, which address the central issues raised by the Information Society, will likely include:

- Building the infrastructure
- Opening the gates: universal and equitable access to the information society
- Services and applications
- The needs of the user
- Developing a framework
- ICT and education

Under each of these broad themes, consideration will be given to the relevant developmental, economic, policy, social, cultural, and technological aspects. A series of preparatory meetings will be held in 2002, beginning with the first PrepCom in Geneva from 1-5 July 2002.

Public-Private Partnerships

The United Nations Development Programme is a member of the Global Network Readiness and Resource Initiative. The purpose of the initiative is to help create digital opportunity in developing nations via guidance in policy, regulatory, and network readiness. The initiative plans to offer country-specific assessment and advice as well as the creation of a Global Task Force that works *pro bono* for developing nation governments and businesses on matters of policy, competition, and electronic commerce. Members of the initiative include the UNDP, the United Nations Foundation, IBM, the Markle Foundation, the World Economic Forum (WEF), and the Center for International Development at Harvard University. Current work of this Initiative was unavailable.

Similarly, the UNDP is also a member of the Digital Opportunity Initiative (DOI), a public private partnership between the UNDP, Accenture, and the Markle. It was launched at the G8 Okinawa Summit in 2000, with the aim of identifying the roles that information and communication technologies (ICT) can play in fostering sustainable economic development and enhancing social equity.

WORLD TRADE ORGANISATION (WTO)

The work of the World Trade Organisation (WTO) in e-commerce has been mostly concerned with matters relating to the take up of e-commerce generally, trade impact and customs restrictions, and Intellectual Property Rights questions. Security considerations have only been identified insofar as they would affect Intellectual Property violations or the imposition of barriers to international free trade.

The WTO defines electronic commerce as the production, advertising, sale, and distribution of products via telecommunication networks. The WTO Secretariat published a background report called 'Electronic Commerce and the Role of the WTO' in March 1998 which examined the potential trade gains to be made via e-commerce. Challenges (including those of security and privacy) were identified, as well as the potential benefits of this new form of trade. The report recognised that the supply of Internet access services and products delivered over the Internet fall within the General Agreement on Trade in Services (GATS).

Issues relating to security and privacy were also contained in this 74-page background report, which can be considered the only declaratory policy statement by the WTO on e-commerce, and associated risks. All other papers and communications have been drafts working towards the e-commerce work plan.

Socio-Political, Economic, and Commercial Overview

The May 1998 Ministerial meeting in Geneva saw the adoption by WTO members of a Statement on Global Electronic Commerce which recognised the growth of e-commerce. The Geneva Declaration, as it became known, mandated a work package involving the relevant WTO bodies to examine issues relating to e-commerce, including the take up of e-commerce in developing countries and taking into account work done by other international organisations. The Geneva Declaration also stated that WTO members should continue their moratorium on imposition of customs duties on electronic cross-border trade.

The General Council's work programme was to take notice of concerns raised by members and produce a progress report to be submitted for review at the WTO Third Session.

This work programme was adopted by the WTO in September 1998. The scope of the work included issues relating to the production, distribution, marketing, sale, or delivery of goods and services by electronic means. Also included was the development of infrastructure (telecommunications and ICT networks) for facilitation of e-commerce. Those carrying out the work were also to consider possible ways of obtaining information from other organisations, to minimise the 'reinvention of the wheel', so to speak.

The main organisations tasked with work in this area were the Council for Trade in Services (CTS), the Council for Trade in Goods (CTG), the Committee for Trade and Development (CTD), and the Council for TRIPS (Trade Relating to Intellectual Property Rights).

CTS was tasked with looking at a variety of issues relating to e-commerce and the work of the WTO within the context of the GATS. These included scope, Most Favoured Nation (MFN) trading status, transparency, participation of developing countries, domestic regulation, standards and recognition, competition, protection of privacy, public morals, the prevention of fraud (under Article XIV of GATS), market access commitments on electronic supply of services (value added telecommunications and distribution), access to public telecommunications networks, customs duties, and classification issues.

The Council for Trade in Goods was tasked with the examination of aspects of e-commerce relating to the GATT (General Agreement on Tariffs and Trade) 1994 and multilateral trade agreements covered under Annex 1A of the WTO agreement. Issues for consideration during the course of the Work Programme were market access for products relating to e-commerce and more general access to such products, issues arising from the application of the Agreement on Import Licensing Procedures, customs and other duties and charges, standards in relation to e-commerce, rules of origin, and classification issues.

The Council for TRIPS was asked to examine intellectual property issues including protection of copyright and related rights, protection and enforcement of trademarks (which included work on Domain Names), and new technologies and access to technology.

Finally, the CTD was asked to examine and report on development issues relating to e-commerce, particularly its effects on trade and economic prospects of developing countries (especially SMEs), means of maximising any possible benefits to them from this new form of doing business, challenges to and ways of enhancing the involvement of developing countries in e-commerce (especially as it relates to the use of e-commerce as a means to integrate developing countries into the multilateral trading system), questions relating to improved access to infrastructure and technology transfer, the implications for developing nations on the impact of e-commerce on traditional means of distribution of physical goods, and finally, any further financial implications of e-commerce.

In June 2001, the WTO Committee on Trade and Development (one of the three bodies looking into this area) held a seminar on Government Facilitation of E-Commerce for Development. During this seminar, four main topics were discussed: regulation and deregulation, promotion of modern ICT (Information Communications Technologies), education and information, and government co-ordination. Another question put forward was identification of the most appropriate legal framework needed to reap the benefits of e-commerce. Directly following this meeting, the General Council held more in-depth discussions at a higher level.

The commitment of the WTO to this issue was reaffirmed in the Ministerial statement at Doha on 16 November 2001, which stated that the WTO would continue its work on creating and maintaining an environment favourable for the future development of e-commerce. The statement concluded that the work done so far demonstrates the new challenges and opportunities for trade that e-commerce presents.

Work on electronic commerce was published by the CTD in its 1999 annual report, where it said that e-commerce was discussed extensively at informal meetings in November and December 1998. Issues discussed revolved around the impact of e-commerce on developing countries and potential benefits and challenges that e-commerce may present.[1]

Analysis of the Main Regulatory and Legal Developments Related to Information and Telecommunication Systems and Services

The agreed definition of e-commerce in the WTO appears to split it into three related parts - Internet access services, electronic delivery of services, and finally, use of the Internet for provision of distribution services (sale of goods and services to be delivered in a non-electronic form).

The WTO believes that market forces cannot be left alone in the development of e-commerce. In particular, government intervention and industry self-regulation were seen as necessary in the following areas:

---

[1] Committee for Trade and Development, *Report to the General Council* (1999): para 14-16

- Security and privacy of data
- Standards for emerging telecommunications infrastructure
- Adequate investment in the existing infrastructure
- User-friendly and broad-based access
- Predictable legal and regulatory environment that enforces contracts and property rights
- Rules for acceptable and conditionally acceptable content
- Predictable framework of taxation and financial regulation
- Equal opportunity through better education in developing and developed countries

Efforts made by the international business community to address these issues have been recognised, but the WTO agrees that targeted government intervention may be necessary in some areas.

However, if the background WTO Secretariat report is any indication, it would seem that too much emphasis will be laid upon encryption as a means of securing.

One can expect that work will be focused on promoting competitive environment to ensure affordable access. This includes the debate over provision of services and pricing (and includes questions relating to telecommunications deregulation, local loop unbundling, etc.) Although the CTG/S agreed that ISP (Internet Service Provider) services come under GATS and that ISPs should be allowed fair and reasonable access to the PSTN (Public Switched Telecommunications Network), they raised questions as to whether ISPs should provide such infrastructure themselves.

WTO discussions have also emphasized the need to liberalise internal markets, market access, and export interest for developing countries. The issue of competitiveness and partnerships between developing and developed countries, and the public and private sector were mentioned as issues for further work. Competition safeguards were also reviewed and WTO councils discussed whether these existing rules could be applied to suppliers of telecommunications services, such as software, certification, and authentication. Delegates were also urged to take note of the exploratory work that was taking place in the Working Group on the Interaction between Trade and Competition Policy.[2]

Existing commitments of member nations under GATS did not need to be adopted for e-commerce. This meant that standing commitments on telecommunications would apply to the use of the Internet as a means to provide telecommunications services and commitments on distribution services could apply to online ordering and delivery of products.

The progress report of the Council of Trade in Goods contained much information regarding definitional issues relating to e-commerce, and whether something purchased online was a product or a service (and therefore what set of WTO rules it should come under). However, the need for international standardisation was emphasised, but that any measures should not become trade

---

[2] *Council for Trade in Services Progress Report of the E-commerce Work-plan to the WTO General Council* (March 1999)

barriers or impediments to the competitive development, transfer, and dissemination of technologies related to the global information infrastructure.

CTG's 1999 progress report on the e-commerce action plan identified a number of issues that delegates felt required further attention. Standards (relating to both the commodity and the medium) were emphasised as a key factor in global electronic commerce. Other issues included the development of standards for software applications, disadvantages arising from the rapid pace of technological change in the infrastructure, encryption technology, dominance of the telecommunications market, compatibility of protocols and hardware, standards for content and the market dominance of a few companies in the ICT sector. This is clearly a broad remit for debate and it remains to be seen exactly how much work the WTO can expect to do on all of these issues, especially with its focused trade remit. Although the idea of a facilitating framework of general principles relating to e-commerce was put forward, delegates to the CTG urged caution in dealing with areas like consumer protection, security, and fraud.[3]

Assessment of Phenomena Undermining Dependability

The World Wide Web presence of the WTO and its uneasy relationship with those who oppose what it stands for has meant that on several occasions, the organisation has become the target of cyber-criminality. Such attacks have included e-mail 'spamming' to effect denial-of-service, web-site denial-of-service attacks, web-site defacements and forgeries, and interruption of virtual town hall meetings (this occurred at a live online press conference in February 2001 where the Director-General, Mike Moore, was forced to cease participation due to electronic 'invasion'). However, spokespersons for the Secretariat have consistently reiterated the strength of defences within the WTO, remarking that many of the attacks were simply 'bounced back'.

In terms of the content of discussions within the WTO, major concern has been raised at a number of meetings about a whole series of issues undermining the take up of e-commerce and online trade in both the developing and developed world. Many of these issues have been identified and discussed by the Committee on Trade and Development, one of the handful of WTO bodies tasked with carrying out work into the e-commerce Work Programme.

Such issues include but are not limited to: the digital divide in developing nations; the problems of infrastructure investment in developing economies (so that they might actively participate in a 21st century global economy); the need for action to address the skills gap; the lack of successful case-studies to use as models; the effects of e-commerce on modes of supply, competition in different sectors, and member obligations and commitments under current WTO agreements; the impact of e-commerce on customs revenue, intellectual property protection, and regulatory regimes.[4]

Work on tackling cyber-security has taken place mainly in the Council for Trade in Services, as part of its mandate under the Global Electronic Commerce Programme. Under this, CTS was asked to look at questions concerning the protection of privacy and public morals, and the prevention of fraud, as specified under article XIV of the GATS (General Agreement on Trade in Services).

Specifically, discussions relating to this were conducted in March 1999, just before the CTS was due to submit its progress report to the General Council.

The Council concluded that any action by Members under article XIV of GATS with respect to the prevention of fraud should be subject to a test of necessity and not be used as an excuse to

---

[3] *Council for Trade in Services Progress Report of the E-commerce Work-plan to the WTO General Council* (July 1999)

[4] Report to the General Council, Committee on Trade and Development, *Work Programme on Electronic Commerce: Contribution by the Committee on Trade and Development – Report by the Chairman* (13 November 2000)

exercise trade sanctions or other forms of low-level 'economic warfare' against other members. The Council tentatively put forward doubts regarding the creation of criteria for the policy objectives identified in Article XIV of GATS and it was suggested at this meeting in March that no further work needed to be done on this as the issues could only be resolved in the context of a dispute settlement.

However, the CTS emphasized the need for all members (especially developing countries) to have access to the most advanced encryption technologies available and that it was an unfortunate fact that access to such technology was often denied. This was in response to a protest put forward by Cuba, which was angry at the continued embargo on exports of technology necessary for the development of e-commerce. CTS delegations did put forward the idea of looking at what policy objectives relating to online fraud and privacy would require regulatory measures restricting e-commerce but doubts were expressed as to whether the WTO was an appropriate forum to do so, especially when the role of the WTO is concerned with 'tackling trade restrictions not that of legitimising restrictions'. CTS delegates were also against the provision of generalised measures citing the difficulty of enforcement given the blurred distinctions between many areas in this field. Finally, the CTS meeting reported that some members said that the WTO should not look to setting specific standards to encourage ecommerce (for instance, security standards like ISO 17799).[5]

[5] Meeting of 22-24 March 1999 of the Council of Trade in Services.