

## Draft WGIG Issue Paper on Cybersecurity and Cybercrime

This paper is a 'draft working paper' reflecting the preliminary findings of the drafting team. It has been subject to review by all WGIG members, but it does not necessarily present a consensus position nor does it contain agreed language accepted by every member. The purpose of this draft is to provide a basis for the ongoing work of the group. It is therefore not to be seen as a chapter of the final WGIG report, but rather as raw material that will be used when drafting the report. This draft working paper has been published on the WGIG website for public comment, so it will evolve, taking into account input from governments and stakeholders.

### Issue (what?)

The WSIS Declaration of Principles recognizes that: “the management of the Internet encompasses both technical and public policy issues ...” One of the public policy issues which require careful consideration is security and crime. Not surprisingly therefore the Plan of Action considers that: “confidence and security are among the main pillars of the Information Society.”

As stated in the Executive Summary of a communication from the European Commission titled Network and Information Security: Proposal for A European Policy Approach Com(2001)298 Final:

*“Network and information security can be understood as the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions. Such events or actions could compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data as well as related services offered via these networks and systems.”*

Such malicious cybersecurity intrusions therefore give rise to cybercrimes, which are described in a 2000 McConnell International report as “harmful acts committed from or against a computer or a network”[Schneider and Hyner Page 6]. On accepting this definition, it follows that the Internet: global network of networks, presents the main opportunity for cybercrimes.

As described in The Electronic Frontier: The Challenge of Unlawful Conduct Involving the use of the Internet, A Report of the President’s Working Group on Unlawful Conduct on the Internet dated March 2000 , cybercrime may be encountered with the computer used as a communications tool, a storage device or as a target itself. Storing pornographic material and physically damaging a computer are examples of the latter two mechanisms. Illegal distribution of racist or sexually explicit materials, intellectual property theft, stealing credit card numbers, and launching computer viruses are all examples of cybercrimes effected over the internet. The internet is heavily dependent on the public telecommunications infrastructure. In several countries, multiple competitive operators provide inter-connected networks which increase the opportunities for security intrusions. Examples of cybercrimes committed through cybersecurity intrusions into the telecommunications network are: illegal access of a PABX, getting dial tone and then dialing for free to any part of the globe, or listening to other people’s conversation.

Now some of these crimes such as fraud, piracy and counterfeiting are really old crimes being committed in new ways. This has led Vice President Gore to state in 1999 that “unlawful activity is not unique to the internet – but the internet has a way of magnifying both the good and the bad

in our society ... what we need to do is to find new answers to old crimes.” Some people do not consider such offences to be ‘cybercrimes’ because they say it is like using a mobile phone in the course of a robbery and that does not make it a mobile phone offence! However, some are distinctly new types of crimes such as hacking and the release of viruses into the network. Schneider and Hyner observed that “the scale, scope and complexity of these problems .... seem to trigger and propel the growth of an array on new institutional arrangements and governance structures geared to deal with these kinds of security issues.” However, the lack of effective coordination remains a challenge.

Another issue concerns the difficulty in detecting and prosecuting most offences committed in a global network. Criminal law is generally limited to the jurisdiction of the state. For example, the Computer Fraud and Abuse Act was created in the United States in 1986 in response to increasing cybercrime, while corresponding legislation was enacted in the United Kingdom by way of the Computer Misuse Act 1990. These statutes have improved the body of law available to deal with cybercrime. Collecting evidence from, and extraditing offenders from other states still remains a significant legal challenge. The Council of Europe Convention on Cybercrime is intended to harmonize laws across states and provide for greater international cooperation in this area. Governments must therefore develop new expertise to deal with these new and complex issues.

Cybersecurity and cybercrime are huge problems. Generally they “compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data as well as related services offered via these networks and systems.” Specifically, these activities cost billions of dollars in losses to firms, undermine consumer confidence in e-commerce, damage people’s lives and reputation through privacy intrusions and threaten to disturb the stable and secure functioning of the Internet.

### **Attribution to category / ies**

Stable and Secure Functioning of the Internet.

### **Assessment of risks and problems: what works, what doesn’t, where are the risks?**

A PricewaterhouseCoopers 2001 survey found that of 3400 European organizations, some 43% expects “that cybercrime would be the biggest and most dangerous form of criminal activity in the future.” [IT Governance 2<sup>nd</sup> edition by Alan Calder and Steve Watkins]. In addition to the estimates lost to cybercrime, there are even greater estimates of e-commerce business not conducted because of lack of consumer trust in on-line transactions. So how are the stakeholders addressing this problem?

It must first be recognized that cybersecurity is a moving target. New technologies are being regularly introduced bringing both new benefits as well as facilitating new techniques for criminal action.

Well informed Government policy initiatives and upgraded laws are in many ways effective but take time which is not available in the internet environment. Consequently, greater reliance is placed on the use of security technology to prevent and/or detect violations. The ITU has defined several security standards such as Recommendation X805. According to the ITU, standards which helps to protect the different layers of the telecommunications infrastructure also helps to

protect content in the “services layer”. In addition, the private sector has developed firewalls, encryption, filtering, optical holograms and magnetic strips to help combat this problem on the internet. Additional tools under consideration include authenticated directories and frameworks for the exchange of authenticated directory information which would facilitate tracking perpetrators of cybercrimes. In addition, it is important that law enforcement officers are provided with the sophisticated tools necessary to function in this high tech environment, and are properly trained. It must be remembered that detection and prosecution works, provided the evidence is clear and the laws do not encounter jurisdictional difficulties.

Nevertheless, one of the most effective tools in the fight against cybercrime lies in the education and awareness of users of computers and networks.

Now what doesn't work?

As suggested above, the costs of cybersecurity failure can be very high. The dependency of modern business and government on the internet is close to being absolute, therefore any risk of confidentiality, integrity or availability failures of the network is unacceptable. The challenges faced in the information society are therefore broadly technical, legal, commercial and social.

As already mentioned, technical innovations are equally exploited by criminals. The challenge therefore is to implement technical solutions which limit the opportunity for criminal exploitation.

Legal challenges relate to search and seizure of data in a computer, decryption of illegally encrypted data, the quality of evidence generally and jurisdiction as mentioned above.

The matter of regulation of the internet is a continuing debate. Self-regulation is consistent with the general trend in Government and private sector in the US while Europe tends to prefer some measure of regulation. Directive 95/94 of the European Union: the Privacy Directive, coupled with the US/EU Safe Harbour agreement clearly demonstrates these differences. In the US, it would appear that greater protection is afforded ‘freedom of information’ than individual privacy. As a result, personal information tends to be relatively easy to access and mis-use of such information or the proper use of erroneous information can cause untold difficulties for the affected individual. However, privacy is much better protected in Europe.

It is noted that on both sides of the Atlantic there is the need to minimize conflicting privacy and security obligations on users and business while accommodating and not impeding effective criminal investigation and prosecution.

However no one tool can be expected to secure a network as extensive and complex as the internet, nor the information carried or stored on it. McConnell International [www.mcconnellinternational.com](http://www.mcconnellinternational.com) discourages reliance on law and recommends focus on people, processes and technology.

### **Actors (who, with whom?)**

In cybersecurity and cybercrime the relevant stakeholders are Government, private sector, civil society and international organizations.

## Government

Governments have full responsibility for the maintenance of law and order within their borders. In Western democracies, the powers of Government are separately located in the administrative, the legislature, and the judiciary arms. So while the administration is responsible for the overall policy that determines Governments strategy and action, the legislature makes the laws while the judiciary independently interprets the law and determines guilt or innocence. One of the administrative functions of Government, however, is the enforcement of the law which is executed through the police and other law enforcement agencies. But even in this area the policy of the US Government to promote self-regulation is evident in a Report of the President's Working Group on Unlawful Conduct on the Internet dated March 2000 which states that:

*“Consistent with the Administration’s overall e-commerce policy, the private sector has a critical role to play in ensuring a safe and secure online environment. The distributed, networked, and decentralized nature of the Internet now means that the “rules of the road” must be global, flexible, effective, and readily adaptable to technological change. In particular, the private sector must take the lead in areas such as the design of new technologies to protect children online, self-regulatory consumer protection initiatives, and coordination and cooperation with law enforcement authorities.”* [The Electronic Frontier: The Challenge of Unlawful Conduct Involving the use of the Internet]

While placing this emphasis on the role of the private sector, the US Government has nevertheless enhanced its legal and technological surveillance strategies in the face of terrorists threats after September 11, 2001.

However, other countries and stakeholders think that the role of the private sector should be tempered with adequate respect for the public interest, as defined by laws, governments and citizens. It must be ensured that efforts to survey the Internet and combat cybercrime are not bound to the private interests of specific groups or countries, but contemplate the rights of all peoples and of the global community of individual Internet users.

## Private sector

Private sector interests are normally vested in a variety of trade associations.

Schneider and Hyner conducted some on-line research which shows the Information Technology Association of America (ITAA) [www.ita.org](http://www.ita.org) is the leading actor in the IT sector in the US with “over 380 corporate members”. “The Association plays the leading role in issues of IT industry concern including information security.” [The Global Governance of Cybercrime: Issue Space and the Transnational Policy Network March 2003]

Another strong private sector actor is the World Information Technology and Services Alliance (WITSA) [www.witsa.org](http://www.witsa.org). Founded in 1971, this global alliance of information technology associations represents some 90% of the world's IT market. Their web site informs that they play an active advocacy role in international public policy issues, encouraging cross-industry and Government co-operation to, among other things, enhance information security. WITSA asserts that the internet must be protected at the international, regional, national and individual level, and publishes some principles to guide the development of future policy.

As in the case of the US Government, its private sector strongly supports self-regulation. More importantly however the private sector is constantly researching and pursuing the development of

innovative technologies and delivering hardware and software solutions that help to detect and prevent certain cybercrimes.

### Civil Society

The Centre for Civil Society (CCS) of the London School of Economics [www.lse.ac.uk](http://www.lse.ac.uk) defines civil society in part as: “*the arena of uncoerced collective action around shared interests, purposes and values....*” Civil society is the term used to represent the variety of organizations working alongside Government and the private sector to ensure progress in areas such as human rights, democracy and sustainable development. However, such groups are known for their skill in attracting public attention in their efforts to influence decision makers. For example [www.statewatch.org/news/oct00/06cyber.htm](http://www.statewatch.org/news/oct00/06cyber.htm) reported in October 2000 that "Members of the Global Internet Liberty Campaign (GILC) today (18 October) urged the Council of Europe to reconsider a draft treaty on "Cyber Crime." The international coalition of civil liberties and human rights organizations said the proposal posed a threat to free speech and privacy on the Internet." Another group, Privacy International, considers that while Governments appear to be trying to combat cybercrime they are in fact pursuing surveillance and control of the Internet.

### International Organizations:

There is no exact equivalent of the above mentioned arms of Government in the international sphere. However there are international forums in which Governments can debate and agree treaties and conventions which may have the force of law if ratified into the domestic law of the state. The UN, WIPO, ITU, OECD, APEC, the Hague Conference on International Private Law, the European Commission and the Council of Europe are some of the inter-governmental organizations playing a role in the development of policies and legal guidelines aimed at curtailing cybercrime.

The Council of Europe, as mentioned earlier, developed a Convention on Cybercrime in 2001 which provides for the harmonization of the laws of its 43 member nations as well as those additional states which choose to sign the Convention. The Convention also provides for the criminalization of harmful acts against ‘computer networks’. President Bush has recommended, and the ITAA has urged the US Senate to ratify this Convention despite some remaining concerns of civil society.

### **Forums (where, when?)**

Cybersecurity and cybercrime issues are being discussed in a wide range of forums covering all stakeholders. Some of these forums, such as ICANN and WIPO, function in specific narrow areas while the others operate with a much wider and possibly unlimited scope.

In Western democracies, the work of Government is effectively open to the public on an on-going basis.

IGO’s discussing cybersecurity and cybercrime include ITU [www.itu.org](http://www.itu.org), APEC [www.apecsec.org.sg](http://www.apecsec.org.sg) and the OECD [www.oecd.org](http://www.oecd.org). The 186 member ITU, with some 650 private sector members, has as one of its goals: “to promote the extension of the benefits of the new telecommunications technologies to all the worlds inhabitants;” while the 21 member APEC is “the premier forum for facilitating economic growth, cooperation, trade and investment in the

Asia-Pacific region”. The OECD, on the other hand, with 30 high income member countries and “relationships with some 70 countries, NGO’s and civil society (it has a global reach”.

ICANN’s [www.icann.org](http://www.icann.org) main concern is with the DNS and IP address management. Both of these areas have security implications for internet users and therefore ICANN’s broad membership forum also addresses cybersecurity issues. Similarly, the ITU’s work in standards, training and capacity building also covers cybersecurity issues which are problematic on the software driven telecommunications infrastructure and emerging NGN. Both ICANN and the ITU conducts regional seminars in this area.

Concern over the ‘digital divide’, the UN established to ICT Task Force [www.icttaskforce.org](http://www.icttaskforce.org) in November 2000 with a mandate which includes to: “open and broaden the international approach to setting standards, regulatory frameworks and governance mechanisms for ICT-related activities, including in areas such as Internet name assignments, privacy, cyber-crime and commercial and financial transactions.” The Task Force meets in different countries on a regular basis.

The Council of Europe is the oldest political organization in Europe. Participation in its meetings is by Foreign Ministers and Parliamentarians from its 46 member states.

With respect to the private sector, as the ITAA is a member of the more globally represented association WITSA, more attention will be paid to the WITSA forum. WITSA arranges regular meetings both for its members as well as for the general public.

Civil society meetings attract very wide participation, generally according to the special interests of the group whether trade unions, consumers, church etc. These NGO’s have demonstrated remarkable skill in networking and influencing the public through effective use of the internet and the media generally. Also, the fight against cybercrime and its potential damaging effects on on-line liberties are the subject of heated debate in countless on-line groups and forums.

The internet is a rapidly changing technology driving a rapidly changing market place with emerging and converging applications embracing and affecting all stakeholders. The need for wide participation and regular if not constant dialogue on cybersecurity and cybercrime is clear. In the final analysis, the effectiveness of the dialogue will be seen in the decisions made and the implementation of those decisions in the interest of the global community.

### **Governance mechanisms (how?)**

- (a) who participates
- (b) nature of decisions

The range of cybersecurity and cybercrime issues being debated includes Government policy, law and regulation, technology, standards and public awareness. These issues are covered at the national, regional and international levels, with some measure of participation by all stakeholders. However, when it comes to decision making, participation appears to be restricted to the members of the respective special interest group. These selected decision areas are more closely associated with stakeholders as follows:

- Setting public policy - Intergovernmental organizations and Government
- Setting standards - Intergovernmental organizations and Private sector
- Crafting laws - Intergovernmental organizations and Government
- Law enforcement - Government

- Regulation - Intergovernmental organizations and Government
- Self-regulation - Private sector and Government
- Technology development - Private sector
- Internet operational issues - Private sector
- Consumer protection - Civil society and Government
- Public awareness - Civil society and Government

The mechanism of discussion, debate and decision making by different stakeholders is fast in some areas and slow in others. The nature of the decisions made may be voluntary (non-binding) or mandatory (binding). In the above list only Government and the IGO's, are known to have the legal capacity to make binding decisions. These IGO's such as WIPO have dispute settlement arrangements which may or may not be binding, while the WTO uniquely has a legally binding Dispute Settlement Understanding.

### **Adequacy measured against criteria / benchmarks set out in Declaration of Principles:**

It is well documented that cybersecurity and cybercrime governance mechanisms must be multilateral if only because the nature of these activities knows no national boundaries. The efforts of Governments and the intergovernmental organizations to which they belong ensures that decisions are implemented across the membership, ie. on a multilateral basis. It is reasonable to state that in Western democracies, Governments have for a very long time been sensitive to the inclusion of private sector views in multilateral negotiations. More recently, the views of civil society have also been embraced. As the Internet blurs the distinction between suppliers and users of on-line services and technologies, civil society has been calling for an increased involvement in technical regulatory issues. It appears that the university functions somewhere between the private sector and civil society. The comparable power and ability of civil society and the private sector to influence Government as the final decision maker may now be of relevance.

Two challenges remain, however, the level of participation by developing countries and the fragmented nature of decision making by different stakeholders in different entities.