

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. This draft working paper has been published on the WGIG website for public comment.

7 April 2005

## Cluster 2 of WGIG Key Issues relating to the use of the Internet

### 1. Issue Cluster 2 consists of 3 groups of issues:

- *Spam, Cybersecurity, cybercrime, Security of network and information systems, Critical infrastructure protection*
- *Applicable jurisdiction, cross border coordination, Exemption for ISPs of third party liabilities*
- *National policies & regulations*

This Template contains a condensation of more extensive background information and descriptions of existing work as well as some considerations for future work in each of the areas that is contained in the Annex. For a full understanding of the statements and conclusions contained in this Template, it is necessary to read it in conjunction with the Annex.

### 2. Institutions (*Which institution or institutions is/are responsible for governing this issue internationally*)

- *Spam, Cybersecurity, cybercrime,:* APEC TEL eSecurity Task Group, ICPEN, IETF, ITU, OECD, The Council of Europe's cybercrime convention, The London Action Plan (LAP), United Nations (General Assembly),
- *Security of network and information systems, Critical infrastructure protection:* APEC TEL eSecurity Task Group, Center for Internet Security, CERT Coordination Centre, IETF, Information Systems Security Association, International Systems Security Certification Consortium, ITU, OECD
- *Applicable jurisdiction(Hague Convention addresses it), cross border coordination, exemption for ISPs of third party liabilities:* none.

*National policies & regulations:* Non applicable

### 3. Relationship to the Internet

- a) **Direct:** The global nature of the Internet may require international legal frameworks, coordination mechanisms or cooperation structures to promote effective and consistent handling of these issues.
- b) **Indirect:** Conversely, the lack of an international legal framework or coordination mechanism regarding Internet related misconducts, for example, may be considered a risk for the stability of the Internet. This is not a universally held view.

### 4. Governance Mechanism

There are two kinds of international mechanisms:

Binding international treaties (usually called *conventions*): When these kinds of treaties are ratified, in some countries their content automatically becomes national law, and in the countries where this does not happen, they must promulgate the corresponding national law.

Non-binding international treaties (usually called *soft-law*): These treaties make *recommendations* to countries to promulgate national laws on the subject of the treaty in a *harmonized* way. Usually this is a first step towards a subsequent binding international treaty.

### 4. Evaluation against WSIS criteria

- a) **Process Criteria:** *(To what extent do the institutions' Internet-related governance mechanisms meet the following criteria, given what could be reasonably expected in light of the governance mechanism used?)*

The nature of the Internet dictates that action can be effective only when it is multilateral, multistakeholder, transparent and democratic. Most, if not all, of the organizations discussed in this paper may be characterized in varying degrees against the criteria. Within the organizations they are, of course, transparent to a great extent. However, transparency and participation from stakeholders outside of the organizations vary.

- b) **Role and responsibility criteria** *(To what extent do the institution's Internet-related governance mechanisms enable the different stakeholder groups to fulfill their roles and responsibilities as defined by WSIS? To what extent to the different stakeholder groups have the capacity to fulfill their roles and responsibilities?)*

- i) Governments: Negotiate the treaties. Promulgate national laws.
- ii) Private Sector: Develop technical solutions and standards that address these issues, need to be consulted regarding policy decisions to ensure consistency with business and technical realities. Engage and educate users in the use of techniques to combat the problems identified in the issues.

- iii) Civil society: Continue development of appropriate Internet technology through, for example, Open Source projects by NGOs and volunteers, to address the issues. In addition, Civil Society needs to be consulted in the negotiations of the treaties and on the technology developed by the private sector. Engage and educate users in the use of techniques to combat the problems identified in the issues.
  - iv) Intergovernmental organizations: Framework for the negotiation of the treaties. International collaboration on enforcement. Dispute resolution.
  - v) Other international organizations: Technical standards, capacity building, international cooperation.
- c) **Outcome Criteria** (*How effectively to the institution's Internet-related governance mechanisms contribute to achievement of the following goals?*)
- i) **Equitable distribution of resources:** Non applicable
  - ii) **Access for all:** Non applicable
  - iii) **Stable and secure functioning:** This cluster of issues is critical for this.
  - iv) **Multilingualism:** Non applicable

**5. Coordination:** (*How effectively is governance of this issue coordinated with governance of other Internet-related issues?*)

Some coordination is done within the ITU, and very little in the other institutions due to the nature of the intergovernmental process (ie OECD members are from particular countries etc) or other reasons.

**6. Overall assessment:** (*What are the points that most need improvement in order to meet the WSIS criteria?*)

In assessing existing mechanisms against these criteria, it is important to bear in mind that almost all of the institutions responsible for addressing, handling or governing the issues included in this cluster are intergovernmental organizations.

None of the existing governance mechanisms for the issues in this cluster meet the Process Criteria of point 4.a) above. Some hold the view that these issues would be better handled with more coordination, sharing of information and involvement of all stakeholders in the processes that are handling them. The need for a global governance mechanism is viewed by some as not being the appropriate solution to handling some of these issues though they may support information exchange and coordination in some cases.

Others recommend that one option is to initiate a process to negotiate a treaty with the full participation of all stakeholders. The treaty is envisioned to be a binding treaty, but if there is no consensus for having a binding treaty, a *soft-law* approach could be used.

It was suggested by some that negotiation could be conducted in the Sixth Committee (legal) of the United Nations General Assembly. The first thing for the UN Member States to negotiate should be the ways in which the other stakeholders will participate in the negotiation of the treaty. Existing conventions, for instance the Council of Europe's Convention on Cybercrime, could be the starting point for the negotiations.

## ANNEX

### Analysis for Cluster 2 of WGIG Key Issues

---

#### **1. Introduction**

This cluster consists of issues relating to the use of the Internet, including spam, network security, and cybercrime. While these issues are directly related to Internet Governance, the nature of global cooperation required is not well defined.

This note provides a framework for assessing the existing bodies of work and arrangements that address these issues against three sets of criteria derived from the WSIS Declaration of Principles and Plan of Action:

Process criteria – the extent to which existing arrangements are multilateral, transparent, democratic and with the full participation of all stakeholder groups;

Roles and responsibilities criteria – the extent to which different stakeholder groups are able to fulfill the different roles and responsibilities recognized by WSIS, by providing the following inputs to the governance process:

- public policy inputs from governments;
- technical and economic inputs from the private sector;
- community inputs from civil society;
- coordination inputs from intergovernmental organizations;
- Internet-related technical standards and relevant policy inputs by other international organizations.

Outcomes criteria – the extent to which existing arrangements could be improved through coordination, communication, building on existing work and other methods.

These different sets of criteria are linked – at least conceptually – in the sense that open, participatory governance processes that enable all stakeholders to fulfill their roles and responsibilities effectively should result in better outcomes. Conversely, deficiencies in governance processes and/or weaknesses in the capacity of stakeholder groups to fulfill their roles and responsibilities will likely result in outcomes that fall short of the WSIS targets.

In assessing existing mechanisms against these criteria, it is important to bear in mind that almost all of the institutions responsible for addressing, handling or governing the issues included in this cluster are intergovernmental organizations. The intergovernmental nature of these institutions and their legal foundations shape and limit the extent to which the WSIS criteria for good Internet governance can reasonably be expected to be applied – in relation to decision-making structures and processes, as well as in relation to the roles and responsibilities of different stakeholder groups.

In assessing these mechanisms, it is also important to bear in mind that very different kinds of governance decisions, using very different kinds of mechanisms, are made in relation to the issues grouped together in cluster three. These decisions and the underlying mechanisms can be conceived as running on a scale from ‘hard’ to ‘soft’ forms of governance, in terms of the results they achieve and the obligations they generate.<sup>1</sup>

---

<sup>1</sup> See MacLean, D.J., “Herding Schrödinger’s Cats: Some Conceptual Tools for Thinking About Internet Governance”, in MacLean, D.J. (ed.), Internet Governance: A Grand Collaboration, New York, UN ICT

As a result, there are significant differences between intergovernmental organizations – and in some cases within them – on the extent to which the WSIS criteria for good Internet governance can reasonably be expected to be applied to specific issues. As the following section demonstrates, it all depends on the nature of the governance decision being taken.

## **Spam**

### **Existing work/mechanisms**

There is no internationally agreed mechanism to address spam. Currently, private software companies offer a variety of spam filtering software. Some require the individual user to “train” them for greater efficiency, while others operate with varying degrees of sophistication. Some governments become involved as in the case, for example, of the Korean Information and Communications Ethics Committee, a regulatory agency, that offers free spam filtering software to Korean Internet users. It has reduced the volume of spam received by its users by 70% to 90%.

There does appear to be a growing consensus that spam will not be solved through any single top-down mechanism. Rather it will take a concerted effort by all actors using a variety of tools from user education to national laws and enforcement means to resolve the multi-faceted issue of spam. This is supported from the experiences and work done by various bodies such as the EU, OECD, ITU, APEC and others. The ITU WSIS Thematic Meeting on Countering Spam in July 2004 concluded that a comprehensive approach to spam would be five-layered, including:

- Strong legislation,
- Development of technical measures,
- Establishment of industry partnerships, especially with Internet Service Providers, mobile carriers and direct marketing associations,
- Education of consumers and industry players about anti-spam measures and Internet security practices,
- International cooperation at the levels of government, industry, consumer, business and anti-spam groups, to allow a global and coordinated approach to the problem.

The European Commission has identified and endorsed a multi-faceted and comprehensive plan that includes the related security issues that are increasingly associated with spam such as attacks on computers and networks, virus propagation, phishing and others. The EU banned spam in the e-Privacy Directive (2002/58/EC). To ensure the effectiveness of the rules and to share experiences with enforcement, the Commission has established a Network of Anti-Spam Enforcement Authorities, CNSA. CNSA meets regularly to cooperate on anti-spam enforcement and has recently agreed to procedures for cross-border complaints.

Other Commission initiatives, such as the Safer Internet Plus program, complement the enforcement activities to empower parents and teachers with Internet safety tools to combat illegal and harmful content as well as spam. The Commission feels that international cooperation to combat spam is essential because of its evolving nature, from simple unsolicited commercial communications to a vehicle for computer viruses that can take control of single computers or entire networks.

---

Task Force (2004) for a more detailed mapping of governance forms and issue areas. Available as a free pdf download at <http://www.unicttaskforce.org>.

At the international level, the Commission participates in discussions at the OECD and the ITU on anti-spam policies and enforcement activities such as consumer education and cooperation with industry on technical solutions. The Commission also engages in systematic discussions with its major trading partners on a bilateral, and sometimes a multilateral basis.

ITU has conducted work on of spam by conducting workshops, surveying existing work and calling on its technical standardization committees to address the issue in cooperation with other bodies such as the IETF. ITU has created a database to gather anti-spam laws worldwide, and to provide a list of the competent enforcement authorities and their contact details. Further, ITU is implementing a series of cooperative activities on countering spam, in the shorter and longer term, to foster international cooperation, to create harmonized policy frameworks to promote the exchange of information and best practices, and to provide support to developing countries. Information regarding these initiatives as well as a review of other international initiatives on countering spam are also available on the ITU's website.

The ITU World Telecommunication Standardization Assembly (WTSA), held in Brazil in October 2004 approved two resolutions relating to future ITU activities in the field of spam: Resolution 51 on Combating Spam and Resolution 52 on Countering spam by technical means. As a follow-up to Resolution 51, a comprehensive report will be presented to ITU Council in July 2005.

The OECD has also organized a number of workshops on spam to further understanding by its member countries. In addition to serving as an information exchange between stakeholders and member states they have formed the basis for developing an OECD work program on spam. An ad hoc experts group has been formed to develop and implement an OECD Spam Toolkit comprised of legislative, technological and self regulatory components.

The OECD membership, however, is limited to only 30 countries and thus is not inclusive at a global level. It is multilateral, and does include the input of many stakeholders in addition to governments through the Business and Industry Advisory Committee (BIAC) and the Trade Union Advisory Committee to the OECD (TUAC). Non-member states may apply for observer status and participate at meetings and workshops. General outreach to non-member states and coordination with other intergovernmental organizations, for example APEC, is expanding.

Because of the need for more extensive stakeholder involvement, the London Action Plan (LAP) to combat spam was formed in 2004. It currently consists of 26 agencies from 19 countries, plus 11 private sector representatives including 3 associations. In addition, the OECD and the European Commission participate in LAP activities. The London Action Plan is an informal international network for spam enforcers and industry representatives. LAP builds relationships between these entities based on a short document that sets forth a basic work plan for improving international enforcement and education cooperation against illegal spam. LAP membership is open to any spam enforcement agency and relevant private sector representatives from around the world and is growing. LAP calls on members to encourage and support the involvement of less developed countries in spam enforcement cooperation. There are no technical requirements to participate; meetings are conducted telephonically via audio-conferencing. There will soon also be a website to exchange information.

APEC is developing a work program on spam. More information on its program may be available following its March meeting.

Several different directions are being explored by the private sector and by technical bodies, especially the IETF, in terms of technical solutions to spam:

#### Authorization and Authentication

- Requiring that each sender is authorized using a DNS mechanism and that each message be authenticated.

#### Accreditation and Reputations

- Senders gain a reputation based on email behavior and filters are capable of rejecting messages based on reputation.

#### Detection

- Solutions based on statistical analysis of message content.

#### Flow Control

- Message flow from sites is controlled.

#### Operational Solutions

- Input and output filtering by operations.

Such technical solutions must be encouraged, as they are necessary to facilitate and to implement policy decisions on spam. In some cases the technical solutions may be very effective, changing the context for governance efforts.

#### **Some considerations for the future handling of spam related policy and practical issues:**

- Recognizing that a consensus global definition of 'spam' may be difficult, many agencies are focusing on cooperation and enforcement mechanisms to stop harmful and fraudulent email.
- There are a growing number of bi-lateral and plurilateral agreements between countries to enforce national anti-spam laws and provisions across borders. Coordinated efforts at such levels may be very effective and, if so, should be evaluated for replicability.
- Legal, policy and regulatory frameworks at the national level need to be in place that encourage continued innovation so that technological solutions to spam can be developed and implemented.
- The use of email for legitimate purposes must be protected.
- Work already underway, for example at the OECD or LAP can be built upon and not recreated.
- Unique aspects of the impact of spam on developing country infrastructure must be considered.
- Communication and coordination between OECD, ITU, APEC as well as between non-governmental organizations that are addressing aspects of spam is important and should be improved.
- Technical work that changes the context for policy decisions should be tracked.

#### **Cybersecurity, cybercrime**

##### **Existing work/mechanisms**

*The Council of Europe's* cybercrime convention creates a common approach to criminal policy aimed at the protection of society against cybercrime, *inter alia* by requiring the adoption of

appropriate legislation and fostering international co-operation. It recognizes the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies. It is a multilateral convention that requires signatory states to comply with and commit to its provisions and implement national legislation that is consistent with it.

Any country can join the convention if particular criteria are met. The involvement of private industry is acknowledged in the convention, however other stakeholders may not find themselves therein.

ITU has also been involved in security work. Current security measures such as public key infrastructures (PKI), are based on ITU-T Recommendation X.509. In the past two years, ITU-T approved two new security Recommendations, E.408 on Telecommunication Networks Security Requirements and X.805 on Security Architecture for Systems Providing End-to-End Communications, and has published a manual titled "Security in telecommunications and information technology".

In addition to technical work in its standardization groups, and educational work in its development sector, ITU has conducted and continues to organize workshops on cybersecurity. A WSIS Thematic Meeting on Cybersecurity June 28 – July 1 2005 at ITU headquarters in Geneva, Switzerland will examine the recommendations in the World Summit on the Information Society (WSIS) first phase's Declaration of Principles and Plan of Action that relate to building confidence and security in the use of ICTs and the promotion of a global culture of cybersecurity.

In the area of online consumer protection, the International Consumer Protection and Enforcement Network (ICPEN) has conducted annual sweeps for consumer fraud. ICPEN is a membership organization consisting of the trade practices law enforcement authorities of 29 countries, most of which are members of the OECD. The mandate of ICPEN is to share information about cross-border commercial activities that may affect consumer interests, and to encourage international cooperation among law enforcement agencies.

### **Some considerations for the future handling of cybersecurity and cybercrime related policy and practical issues**

- Ensure similar criminalization of specific cybercrimes and crimes committed in cyberspace on a global level, respecting the diversity of cultures and legal systems, to avoid the creation of "cybercrime havens".
- Different nationalities have different legal systems and criminal laws; therefore, arrangements and cooperation mechanisms between enforcement agencies are the appropriate way to deal with cybercrime that crosses borders.
- Accommodating and not impeding effective criminal investigation and prosecution consistent with appropriate protection of privacy.
- Adopting clear procedural safeguards consistent with appropriate privacy protection for the interception, preservation, production and seizure of data to ensure the efficient and expeditious response to law enforcement requests, including a safe harbor for cooperation with law enforcement.
- Human rights conventions and treaties need to be respected; i.e., anything that is guaranteed as a human right cannot be criminalized.

- Countries that are not prepared to sign and ratify the Convention may nevertheless consider using it as a basis for strengthening their legal framework for dealing with the cybercrimes addressed by the Convention.
- Develop non-binding guidelines based on the COE convention principles and commitments to allow non-signatory states to introduce measures that help to prevent and address cybercrimes without going through the signatory and ratification processes.

## **Security of network and information systems**

### **Existing work/mechanisms**

The first line of defense in many countries is the CERT (computer emergency response team) when there is a breach, potential or otherwise, in computer security. CERTs are typically made up of technical experts who are in communication with other CERTs to share knowledge and best practices and to warn of impending attacks. In some countries these CERTs are part of a government department; in other countries they may be in private sector organizations such as commercial companies or universities. Many CERTs belong to the Forum of Incident Response and Security Teams (FIRST) as membership enables a more effective response.

The OECD, as part of its security initiatives, issued revised guidelines for the Security of Information Systems and Networks: Towards a Culture of Security in 2002. The current Guidelines consist of nine principles that comprise a framework for considering security issues. The Guidelines address the evolving risks and greater interconnectivity of a networked economy. Virus and other attacks that can disrupt business as well as interfere with the critical infrastructure and physical security, have placed security among the top concerns of business, government and civil society. The OECD Guidelines promote the need for a holistic approach, involving all stakeholders, towards information security by directing the guidelines to ALL participants, as appropriate to their roles. The foundation principles focus on the need to be aware of risks, the need to take responsible action related to those risks and the need to coordinate that action in timely response. The social principles address issues related to behavior, fairness, openness, transparency and values. The last four are more operational in nature and address the “security lifecycle”.

As noted above under “Cybersecurity”, ITU also has an active security program.

In addition to existing EU legislation on security, the European Network and Information Security Agency (ENISA) has been established to ensure network and information security within the European Community. The Agency aims to contribute to the development of a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organizations of the European Union.

The IETF has done and continues to do a significant amount of work on developing security protocols. It requires that all protocols it approves for standardization be securable, ie protocols must undergo a security evaluation before being brought out. However, vendors often do not implement the security mechanisms, or users ignore the tools available. Use of the security mechanisms is always optional.

### **Some considerations for the future handling of security of network and information systems related policy and practical issues**

- Security requires a holistic approach with each participant undertaking measures appropriate to their role; understanding that there may be principal spheres of influence and that collaboration on many levels will be required. A standardized approach to information security may undermine the level of network security.
- Stakeholders must be able to implement an approach appropriate for their needs and risks.
- A standardized approach can have several negative consequences:
  - Stifle the development of innovative technologies and practices by creating a ceiling rather than a floor.
  - Increase vulnerabilities by informing potential hackers how systems are protected- and therefore how they can break into these systems
- Information system security must be proportional. Inherent in the concept of proportionality is the need to assure that the administrative burdens of record keeping and compliance do not result in unintended consequences that impede the use or deployment of security technology.
- Governments have a strong role to play in raising awareness and to educate all stakeholders about the importance of properly configured systems and available network protection tools. Governments should exchange and share such information regularly.
- ITU-T Recommendations and OECD guidelines should be explored for suitability to serve as the basis for coordinated efforts at the national, regional and international levels.

## **Critical Internet infrastructure protection**

### **Existing work/mechanisms**

Various Internet-specific entities have been established with the primary goal of ensuring the stability and security of critical infrastructure. Among these are the IETF and operators' groups such as NANOG, APNIC and RIPE. In these groups, threats to stability and security are considered and resolutions, both in terms of protocols and operational methods, are proposed and deployed.

In many countries, the telecommunications network is a key component of the Internet infrastructure. Within ITU, work on protection of critical infrastructure takes place in the context of the security work described above in the section on Cybersecurity, and also within ITU-T Study Group 6 (Outside Plant and related indoor installations). This work is carried out by operators and manufacturers in cooperation with concerned government agencies.

Work is ongoing to find technical solutions, though of course it is a policy decision to figure out how the technology will be applied once it is developed.

### **Some considerations for the future handling of critical infrastructure protection related policy and practical issues**

Many of the considerations under Security are also applicable here.

### **Applicable jurisdiction, cross border coordination**

#### **Existing work/mechanisms**

The Hague Conference on Private International Law is drafting a Convention on Exclusive Choice of Court Agreements that will focus on choice of court provisions between businesses (B2B). This convention has the potential to achieve more predictability and certainty in international contracts within a reasonable time frame and to become valuable for companies engaged in cross-border transactions.

### **Some considerations for the future handling of applicable jurisdiction, cross border coordination related policy and practical issues**

- The Internet is a global medium that is open across all frontiers, and once posted, a website is global from the outset. Likewise, transactions, as well as commercial and promotional material on websites become global.
- Jurisdictional ambiguity is harmful to the information society. First, many goods and services are held back entirely from the global electronic marketplace. Second, other goods and services are offered only in a limited number of jurisdictions, and consumers in other places are denied access to competitive products and prices through the online marketplace.
- Of particular importance is the stifling effect that this would have on small business and the severe limitations it would place on emerging entrepreneurial ventures in developing economies. Clearly the costs and complexities of compliance for these players could preclude their participation in an information society.
- Governments should take care to avoid creating unpredictable grounds for asserting jurisdiction over e-commerce activities.
- B2B and B2C transactions present different issues and concerns. The appropriate fora and mechanisms to handle these issues therefore also differ.
- In the case of business-to-business (B2B) transactions across borders, there exist established conventions and solutions, which help guide such transactions. Contracting parties are usually more sophisticated and often incorporate choice of law and choice of forum clauses in their agreements. There are also well-established arbitration and mediation options to avoid litigation in the courts of one party's country. Party autonomy must be respected in such transactions.
- The work of the Hague Convention should be built upon to ensure the necessary legal, policy and regulatory frameworks are in place at a national level.
- This issue may be best followed through the Hague Convention process.

### **Exemption for Internet intermediaries from third party liabilities**

#### **Existing work/mechanisms**

There are no current international mechanisms that treat this issue.

Exemption of Internet intermediaries such as ISPs, portals and entities that merely transmit content are typically considered within the context of e-commerce enabling laws.

### **Some considerations for the future handling of exemption for ISPs of third party liabilities related policy and practical issues:**

- Discussions regarding these issues need to include all stakeholders at the national, regional and international levels. The World Intellectual Property Organization (WIPO), aware of the impact of the issue on its members, has begun to hold seminars on the issue.
- Best practice continues to evolve and countries can learn from each other.

### **National policies & regulations**

National policies and regulations are the realm of national governments, in consultation with other stakeholders. The principles do not really apply to this issue area with the exception of the need for some harmonization and possibly a forum for discussion and exchange of information and experiences to guide national policy and regulatory decision-making to maximize a country's ability to interact using ICTs and the Internet across borders.

ITU's Development Sector (ITU-D) publishes extensive information regarding national policies and regulations. Information is published by country, and case studies and comparative analysis are also available. Topics cover the full range of national regulatory activities, including, for example, spectrum management, numbering issues, pricing and costs, universal service, unbundling, licensing, interconnection, quality of service, consumer issues, dispute resolution, etc. Workshops are held regularly and a regulator's discussion list (hot-line) permits regulators to ask specific questions and obtain answers from their peers in other countries.

### **Overall coordination and assessment**

- All of these issues would benefit from the exchange of information and some form of cooperation/coordination
- Coordination of national legal, policy and regulatory provisions that relate to all of these issues, amongst national bodies/agencies handling them and importantly between countries is essential.