Comments on WGIG Issue Paper on Cybersecurity and Cybercrime

February 11 , 2005

Authors/Organizations

Fundación Vía Libre

Free Software Foundation Europe

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.

As a comment on the process for accepting comments to WGIG papers, we must point out that just two weeks to review a large number of papers that were written over a period of several months are just not realistic. In an attempt at providing as much constructive criticism as possible in the little time allotted, we are submitting comments to this paper in a "raw" form of gathered comments, instead of the more polished format and wording we would have preferred.

As a general comment to the paper, it is too vague, and contains a large number of factual and conceptual errors. It also spends a lot more time considering issues of enforcement, prosecution, evidence gathering and even extradition than it does looking into prevention, responsibility and protection of internet users from law enforcement abuse. This is a dangerous imbalance.

It is extremely hard to decide to which extent "cybercrime" really is an "internet governance" issue, particularly since we're lacking a definition of what we are choosing to call "internet governance". If we take into account the fact that the criminal nature of any given act depends on the jurisdiction where the act has taken place, it seems that "cybercrime" as an "internet governance" issue would be one of "how do we enforce existing criminal law on the internet?". Unfortunately, attempting this in an inherently multi-jurisdictional medium such as the Net is and extremely thorny endeavour. We must not forget that one and the same act can be criminal in one jurisdiction, while perfectly legal where the person committing the act lives. So if there are going to be mechanisms to enforce law on the Net, which set of laws are we going to enforce? We may choose to enforce the union set of all activities that are considered criminal in any one place of the world. This would mean, for instance, that the internet mechanisms needed to support censorship according to some country's laws would also apply to all internet users living anywhere, which would be inconstitutional in many countries. Or we may choose to enforce the intersection of all the sets of illegal activities, which very well may end up being empty, or not even worth bothering.

We want to stress that this comment is not an appeal for "self-regulation" of the issue, but rather for the freedom of each jurisdiction to regulate the net as it deems best, instead of having a supranational "internet government" dictate paralegislation without due process or representativity.

Of course, there are activities that are not mere computer-aided versions of existing illegal activity, but rather illegal conduct that is novel and unique to the internet, and is only possible within it. These activities, pure "cybercrime" could be a good target for an internet governance body to tackle, provided that it does so with heavy involvement of the user community as its constituency.

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."

We'd like to stress the technical nature of this definition: it talks about the ability of an information system to resist accidental events or malicious actions. It is implied in the definition that the system resisting the events is the target of the attack, and not its source. According to this definition, network and information security are all about technical measures meant to protect the system from accidental or malicious attacks. Prosecution, evidence gathering powers and such are not part of network and information security. At most, they are much less important than proper technical security. It is somewhat puzzling that some positions within this paper fail to reflect this wisdom.

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.

There is a potential problem with the word "cyber**crime**" in this paragraph. In order for an action to be considered a "crime", it is not enough that someone regards it as "harmful". It has to be in violation of an existing law. As a matter of fact, only acts that violate an existing law can be considered criminal, regardless of whether they are harmful or not (the amount of harm done will probably affect the penalty, but the criminal nature is not affected by it).

Of course, the Net gave rise to a range of new harmful activities that are unique to it, and thus were not taken into account by pre-Net legislation. These activities must be first codified as offenses in the law before it becomes correct to speak of them as "crimes".

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.

This paragraph contains several inaccuracies and factual errors:

- besides the unclear and moving definition of "pornography", storing pornographic material is legal in many jurisdictions, and is thus a very poor example of "cybercrime". Not to mention that storing pornographic material can be done without computers, as people have been doing for a very long time.
- physically damaging a computer is usually penalized as vandalism or destruction of private property, and is rarely if ever made easier by the Internet, so it's a bad example of "cybercrime". A better one would be "remotely disabling or interfering with services offered by a computer or network, without proper authorization". Note that this can be achieved even without attacking the system offering the services itself. For example, it can be done by filtering key packets from the system's communications stream.
- racist and sexually explicit material are legal in many jurisdictions, and hardly unique to the internet. They make poor examples of "cybercrime". A better alternative would be "illegal distribution of restricted material", but its lack of uniqueness to the online environment still makes it insatisfactory.
- There is no such thing as "intellectual property theft". Some people incorrectly use this term to refer to different kinds of **infringement** (not theft) on certain state-granted monopolies such as copyrights, trademarks, patents, geographical denominations and others. Infringement of these monopolies is hardly new, and therefore a bad example of "cybercrime". As a matter of fact, the internet is not particularly useful even as a facilitator for most of them. There is no way, for instance, to use the internet to infringe on a patent (unless it's a US-style "doing *X* over the internet" patent, in which case it is arguable that **granting** the patent in the first place was criminal upon society). The internet does facilitate certain types of copyright infringement, so maybe the author meant to write "copyright infringement".
- it should be noticed that the internet also enables copyright holders to deny rightful users access to works they have acquired. It even enables the holders of the copyright of a program to restrict access to data stored using that program, even if they don't hold any rights on the data itself, so "abuse of protective measures" could be another fine example of cybercrime.
- credit card numbers were "stolen" long before the internet existed, using a variety of means. Again, this is a poor example.
- releasing computer viruses into the wild is a good example of pure "cybercrime". There are others which should be considered, such as:
  - knowingly refusing to fix security flaws in software the user has obtained legally, while forbidding or obstaculizing his attempts to fix them himself
  - knowingly releasing software with hidden functionality or intentional security flaws such as back doors, spyware and others
- the issue of intent is missing in this whole paragraph. People may inadvertently get dial tone an talk for free due to a mistake on the telecom operator's part. Or they may listen other people's conversations due to addressing errors, or because they are performing troubleshooting operations on the communications infrastructure. Intent and knowledge are important components of criminal activity.

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.

This paragraph correctly identifies the issue of separating ordinary illegal behaviour that uses information technology as an aid from behaviour that only becomes at all possible through the use of such technology. Unfortunately, the rest of the paper does not derive enough wisdom from this insight.

This paragraph also contains two important inaccuracies:

- the word "piracy" describes an act of violence at high seas, and has meant this since before there was electricity, let alone computers. In this context, the term is probably being used in a colloquial sense that draws an odd parallel between copyright infringement and piracy. This colloquial use is uncalled for in an official paper like this, which must aim for accuracy. It is also too broad, since the definition for the colloquial use of "piracy" is ill-defined and changes over time. We propose to replace "piracy" by "copyright infringement".
- the work "hacking" does not mean what the author thinks. "Hacking" is used by different people as a name for a very broad range of activities, some of them harmful, but most of them beneficial or at least harmless, and only a very small set of them are illegal. For instance, most programming work is talked about as "hacking". A very common meaning of the noun "hack" is "an elegant solution to a non-obvious problem". It would be unwise to declare that innovation is a crime. The author probably meant to write "unauthorized harmful access".

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 Unites Sates in1986 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.

This difficulty is real but, as programmers like to put it, "it's not a bug, it's a feature". If an activity is legal in jurisdiction A, but illegal in jurisdiction B, it's not right for jurisdiction B's justice to be able to demand extradition or prosecution of jurisdiction A's citizens for engaging in it. The solution to this "problem" is not to demand more powers for extrajurisdictional action, but to encourage discussion and consensus on which activities should be regarded as illegal.

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.

The claims in this paragraph seem insubstantiated. It is likely that viruses, trojans and other security problems cost companies large amounts of money, but there again these costs could be reduced drastically if these companies would take some basic security precautions and if software vendors took security as a real issue, instead of trying to sweep it under the rug.

Some activities do undermine consumer confidence in e-commerce, but it is not easy to see how this is an "internet governance" issue instead of a problem that must be dealt with by e-merchants.

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 2nd edition by Alan Calder and Steve Watkins]. In addition to the estimates lost to cybercrime, there are even greater estimates of ecommerce business not conducted because of lack of consumer trust in on-line transactions. So how are the stakeholders addressing this problem?

We fail to see how "ecomerce business not conducted" is an internet governance issue, and not a commercial one.

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.

To say that firewalls, filtering and encryption have been developed by the private sector is wrong. Many of these products, and even their underlying principles, have been developed by public universities, individuals working in free software projects, government research programs, etc.

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

This is an extremely important issue, which deserves more than a single sentence. Most internet users, for instance, are unaware that viruses are **not** an inevitable fact of life, and that technological choices affect the extent to which they are exposed to them and other hazards. They are also typically unaware of the extent to which programs that are distributed without source code are more likely to contain spyware and back doors than programs that are free for anyone to inspect. Most users are even unaware of the extent of a computer program's ability to do things behind the user's back. This lack of awareness causes them to take uninformed choices, or even to ignore the fact that they have a choice at all, and increases the potential for security breaches that affect them personally and the net as a whole.

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.

The challenge does not end there. The technical solutions must limit the opportunity for criminal exploitation **while preserving the full potential for legitimate exploitation**. If the implementation of a given technical solution in order to limit criminal explotability of a feature of the network means that some legitimate exploitation would be hampered too, the technical solution must be deemed unacceptable.

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.

Given that without the right to communicate through encrypted channels and to store encrypted data no security or privacy is possible on the Net, it is not easy to understand exactly when data has been "illegally encrypted".

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 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.

This paraggraph flagrantly omits internet users as relevant stakeholders. Individual users are vital to the Internet, and they ought to be recognized as such.

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.itaa.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. 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 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 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.

Missing organizations here are the Electronic Frontier Foundation, as well as the Free Software Foundation, Free Software Foundation Europe, EPIC and many others.

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, APEC www.apecsec.org.sg and the OECD 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 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 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

To attribute technology development to the private sector only is a gross mischaracterization of the facts. The very Internet was developed as part of a government research program. The standards, protocols and formats underlying the WWW were developed at CERN. The Free Software Foundation as well as numerous individuals have provided operating systems and software components that enable the operation of networks and servers, such as the GNU/Linux operating system or the Apache web server, which holds over 60% of the web server market share.

For contrast, the private sector's efforts to enable computer networks before the Internet, resulted in a dozen incompatible and non-interoperable network standards, none of which ever reached the level of flexibility and richness of the publicly-developed internet, all of them justly forgotten.

The private sector does develop technology, but it's not their prerogative, Technology is developed to the same, if not much larger extent, by governments through research grants, by civil society and by individual internet users.

•Internet operational issues—Private sector

The operation of the internet is not restricted to the private sector. Some countries may wish to operate a state-run network. Civil society, cooperatives and even individuals operate portions of the net outside the "private sector" sphere. Certain operational aspects of internet operations, for instance the management of root DNS servers, are arguably not ideally suited for being handled exclusively by the 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 thelegal 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.