IGF 2010 – Vilnius

Report of Workshop 123

Legal Aspects of Internet Governance:
International Cooperation on Cyber-security
This Report is available at:
http://www.intgovforum.org/cms/component/chronocontact/?chronoformname=WSProposalsReports2010View&wspid=123

Workshop Description.

Globally, in the past few years, concerns have increased sharply over cyber-security, including the issues of cybercrime, "cyber-war," "cyber-defense," "cyber-terrorism," critical infrastructure protection, and information security. At the same time, growing attention is also being paid to how responses to cyber-security may affect, and how they should be balanced with, human rights values, such as individual autonomy, privacy, anonymous political speech, freedom of expression and freedom of association, human development goals, including access to knowledge, and economic interests, including innovation, competition, and the protection of trade secrets and other proprietary information. These issues of policy and values also present complex technical issues, such as the issue of "attribution," that is, the extent of the ability to determine the true senders of any message or request for information. Recognizing that cyber-security contributes to economic development and social cohesion, this Workshop explores the legal aspects of cross-border cyber-security efforts that address the tensions among these conflicting concerns.

Vint Cerf, VP & Chief Internet Evangelist at Google opened the session with a key note speech. Hank Judy, Of Counsel at law firm K&L Gates, gave an overview of the Workshop's Background Paper (attached to this Report). The Workshop then moved to get the perspective of regional organizations. Ivalo Kalfin, Member of European Parliament, gave a European perspective. Rolf Weber, Professor of Law at the University of Zurich and representing the Council of Europe (CoE), gave a perspective current and future work of the CoE. This was followed by Alexander Seger, Head of the Economic Crime at CoE, who focused on the CoE's Budapest Convention. The Workshop then moved to here the perspectives from different countries of their experiences and observations. Jayantha Fernando, Director/Legal Advisor at ICTA Sri Lanka, started off, followed by Erick Iriarte, Partner at law firm Iriarte & Associates in Peru. Andrew McLaughin, Deputy U.S. Chief Technology Officer of the Executive Office of the President US concluded the country section. The Workshop then heard the perspectives of industry and civil society. This part of the discussion was opened by Mike Silber, Member of the Board of ICANN. Bill Smith, Technology Evangelist at PayPal then spoke. John Morris, Director at the Center for Democracy and Technology concluded the Workshop. The Workshop was moderated by David Satola, Senior Counsel, at the World Bank.

The Workshop was organized by the following organizers: Affilias, American Bar Association, Center for Democracy and Technology, Council of Europe, Diplo Foundation, ICANN, ISOC Bulgaria, ISOC Pacific, LACTLD, Oxford Internet Institute and the World Bank.

The Background Paper for this Workshop is attached, below. Also attached are the individual presentations by some of the Workshop panelists. All documents are also available at the following url: http://www.afilias.info/igf10-ws-123 .

Because these are available as part of this report, this report takes a synthetic approach, summarizing the interventions of panelists along thematic lines, rather than attempting to summarize each panelist's intervention. The requested format of the Workshop report does not necessarily lend itself well to capturing the richness of detail of a two hour workshop. Necessarily some of this richness will be lost in the process of synthesizing a wide range of views from panelists representing an equally wide range of stakeholders. Accordingly, any errors, omissions or mischaracterizations of opinions or issues is entirely the fault of the author, and no organizer or speaker (or the organizations they represent) bears any responsibility for any such error, omission, etc.. In this sense, the views expressed in this Report do not necessarily reflect a consensus view among Workshop panelists, but an attempt by the author to capture the range of discussion.

Main Themes.

This Workshop was about identifying opportunities for enhanced cooperation on cross-border legal issues affecting cyber-security. Of course there are numerous examples of existing cooperative initiatives, and CoE's Budapest Convention is but one example. However, the purpose of the workshop was attempt to view these opportunities for enhanced cooperation through a different lens.

In his keynote address, Mr. Cerf provided the citizen-centric, volunteer fire brigade as an analogy for one way in which to address cyber-security issues. When a house is on fire, anyone can call the fire department, and the fire department will do what it can to put out the fire, contain the fire and minimized fire damage to the house. This analogy of loss-minimization (in addition to prevention and detection) was carried throughout the Workshop. National CERT's play this role in part, and achieve an international cooperation through FIRST, for example. The analogy provided a useful foil around which the Workshop was galvanized.

A disaggregated and deconstructed approach better understand Cyber-security.

The first cross-cutting theme that emerged during the Workshop was that in order to better understand issues of cyber-security, and therefore our ability to respond to them, requires us to deconstruct and disaggregate the issues. In its most obvious form, cyber-security must be distinguished from cybercrime and cyber-war. All three may share some common elements and even overlap in the fashion of a Venn diagram, but differences among them also exist. It was noted in this regard that even the term "cyber-war" can set the wrong tone for the debate; and that the term cyber-crime, in itself, could de-escalated a particular threat, without actually

changing the nature of the threat. Participants also expressed reluctance to characterize uses of force involving use of ICTs as acts of cyber-war if only because of the problems of attribution, that is, the ability of initiators to disguise the origins of the use of force. In general they preferred to apply a combination of defensive actions, diplomacy and resort of criminal processes. They nevertheless recognized the reality of cyber-war preparations, defenses and past actions. In some cases this disaggregation is done in a layered fashion. In that vein, network security (the infrastructure layer) could be distinguished from protocol security (the software layer) and from applications security (the applications layer). Cyber threats can be cyber attacks, but can also be the result of "mistakes" or even natural disasters. Similarly responses can be viewed as preventative (ex ante) or loss-minimization (ex post). Even among ex post responses, there are at least two types, emergency fixes (loss prevention) and forensic analysis. New paradigms in international law such as shared responsibilities of states to ensure the protection of critical internet resources should be discussed. One size does not fit all.

Vulnerabilities

The Workshop discussed a number of causes of vulnerabilities. Among these were:

- *Dissonance in national approaches to cyber-security*. Different countries, even members of regional organizations, can take different approaches to the concept of cyber-security in terms of the national policies, laws and implementation. This can lead to a lack of effective coordination. It was also observed that this dissonance resulted in part because of a lack of multi-stakeholder participation in both policy making and legislation.
- *Policy and implementation incoherence* . Even in countries there can be a disconnect between upstream policies promoting an "e"-agenda and the downstream protections of rights and property.
- *Outdated legal architecture that doesn't fit cyberspace well*. Cyber-security is a 21st Century problem that requires 21st Century responses. However, in the legal sphere, many concepts simply do not apply, or cause friction when applied. For example, the lack of consensus on the fundamental and related issues of jurisdiction and sovereignty make it difficult to effectively cross borders to address cross-border incidents. Jurisdiction is used in the sense of the legal capacity to make laws applicable to particular persons and events within a territory and to compel legal process and enforce laws with respect to such persons. Sovereignty is used in the broader sense of the total independent power of a nation state. A nation state may view its sovereignty as being impaired if another nation state may exercise jurisdiction within its borders. However, nation states may view their sovereignty as being enhanced if by mutual agreement they obtain jurisdiction within each others' territories. In order for the rule of law to prevail the inherent cross-border nature of cyberspace seems to require such agreements for the mutual expansion of jurisdiction.
- *Buggy code, bad practice*. There are a number of easily identifiable problems that could be addressed. These include issues with software code, human error and behavioral problems.
- *Existing tools and instruments not fully applied and partial implementation of existing agreements.* Where there are regional or international instruments, they are many times not fully applied or are partially implemented

Balance / proportionality issues

Accordingly, a number of balances emerged. Perhaps the most basic balance is that between ensuring security on the one hand and protection of rights. In this sense, cyber-security should not be used a pretext for restricting rights. Another example is that when dealing with cyber-security incidents, one needs to address both prevention as well as repair and damage limitation.

Finally, there is a balance to be struck (or a trade-off recognized) between legitimate efforts by governments to promote security through application of laws and legal process and the potentially negative impact this may have on promotion of innovation and competition.

Findings and Recommendations

Extracting from the discussion of the Workshop, following are some of the key outcomes and recommendations for enhanced cooperation going forward:

- *Layered approach.* Cyber-security should be approached in a layered fashion.
- *Resiliance vs. perimeter security*. Concepts of security based on "securing the perimeter" applicable in past decades to closed systems should be reviewed in favor of concepts of surety based on resilience (flexibility of response to type of threat and ability to recover and adjust more quickly to changing threat environments).
- *Identify incentives.* A range of incentives (including economic and behavioral incentives) exist that should be (i) understood and (ii) employed in the design of security response systems. This could even include identifying innovative incentives to change behavior of users, such as an insurance market, that could accurately price the risk of security.
- *Fully implement existing instruments.* It was argued that many tools, instruments and good practices are already available to help societies cope with cybercrime, including the Budapest Convention.
- *Increase awareness and build capacity* , including especially of policy makers, legislators, regulators and law enforcement personnel.
- *Ensure cyber-security needs are adequately resourced*. (see above)
- *Create cyber-security accountability*. In some countries an accountable cyber-security "czar" is named, but in others, or in systems with diffuse accountability, lack of clear identification of responsibility can lead to vulnerability.
- *Law Reform.* Here there were three areas meriting mentioning: first is that in developing countries, a robust, comprehensive law reform component should be included in development projects; second, national laws should drafted with a view towards achieving, if not harmonization, then interoperability across borders; and third, international law responses can provide for improvements of the functioning, stability, and resilience of the Internet.
- *Sovereignty issues may require re-examining existing concepts of the "State"*
- *Use of PPP models and approaches*. Recognizing that no country or entity can address cyber-security alone, governments should be encouraged to work with industry and civil society in addressing cyber-security needs. Indeed, the private sector, since it owns much of the infrastructure and since it has resources and incentives for security, should be actively engaged, perhaps through a variety of public-private partnership models.