

Overview Of Background Paper
and a Personal Suggestion
Legal Aspects of Internet Governance:
International Cooperation
on Cyber-security

Vilnius IGF Meeting - Workshop 123
Wednesday, September 15, 2010

Henry L. Judy, Esq.
K&L Gates LLP
Washington, DC 20006
USA
henry.judy@klgates.com

Workshop Theme

- Sharply increased global concerns over tensions among:
 - cyber-security issues
 - Protection of human rights values and human development goals
 - Protection of vital economic interests
 - Addressing complex technical issues involved, such as the issue of “attribution”
- Explore legal aspects of cross-border efforts that address the tensions among these concerns

Background Paper Outline

I. Recent Developments Prompting Heightened Concern

II. International, National and Organizational Responses

A. Cyber-crime – The [Law Enforcement](#) Response

B. Building and Defending More Secure Networks – The [Governmental and Corporate](#) Response

C. Cyber-War – The [Military and Diplomatic](#) Response

D. Structuring [National](#) Responses

E. [Economic](#) Concerns

F. Promoting [International Cooperation](#) on Cyber-security

Exhibit A - Selected Bibliographic References

Recent Developments Prompting Heightened Concern

- Increased appreciation of **criticality of the Internet** in multiple spheres of human endeavor and activity
- Continuing disclosures of **major data breaches**
- Continuing releases of more sophisticated **malware**
- Continuing reports of varying levels of governmental **monitoring and filtering** of Internet use and content
- Cyber-attacks on key infrastructure in various countries
- Concerns with governmental and corporate **espionage**
- Increased concern over **cyber-crime** and related **criminal money flows**
- **Privacy concerns** with corporate and governmental data access

Cyber-crime – The Law Enforcement Response

- Several instruments have emerged to deal with **directly** cyber-crime internationally, such as
 - The Council of Europe’s (COE) Budapest Convention
 - The Commonwealth of Nations’ Model Law on Computer and Computer Related Crimes
 - International Telecommunications Union’s draft cyber-crime legislation
- Other efforts are **indirect** such as by re-examining privacy laws
- Over 100 countries have some form of cyber-crime legislation, often based on the Budapest Convention
- At the recent UN Crime Congress efforts to negotiate a global cyber-crime treaty were unsuccessful

Cyber-crime – The Law Enforcement Response

- Questions for consideration include:
 - how these disagreements can be bridged
 - need to balance different interests, rights and values
 - impact of rapidly developing technologies
 - local limitations of resources and expertise
 - existence of nation states that serve as “safe havens”
 - what the dynamics and incentives are for a nation state to maintain “safe haven” status

Building and Defending More Secure Networks – The Governmental and Corporate Response

- Critical infrastructure is in three hands:
 - private sector
 - governments and quasi-governmental entities
 - effectively both because of the extensive connectivity between them
- Responses include, on a national and international basis
 - the work of [international standards bodies](#)
 - ICANN's promotion of security extensions for the domain name system ([DNSSEC](#)).
 - Continuing development of Computer Emergency Response Teams ([CERTs](#)) for information sharing and better coordination among government agencies and the private sector and respond to cyber-attacks

Building and Defending More Secure Networks – The Governmental and Corporate Response

- Issues include:
 - Should protections for governmental networks be extended to privately owned networks or should the private sector manage its own intrusion detection and other security systems?
 - Should extension be legally compelled?
 - How to delineate which are covered and which are not
 - How are privacy and confidentiality maintained?
 - Legal effects of trans-border data flows
 - Third party auditing? Quis custodiet ipsos custodes?

Cyber-War – The Military and Diplomatic Response

- International Cyber-War Treaty?
 - January 2010, ITU Secretary General Hamadoun Toure proposed world's nations should adopt a treaty in which they would engage not to make the first cyber strike against another nation.
- Recent NATO experts report
 - included recommendations for changes in the NATO Strategic Concept to specify the characteristics of a cyber-attack that would trigger the obligation of collective response under Section 5 of the NATO treaty.
- Article 51 of the UN Charter
 - “Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations.....”
 - The application of Article 51 with respect to cyber-war has been hotly debated in the academic literature without any firm conclusions being drawn.

Cyber-War – The Military and Diplomatic Response

- How does the “law of war” – including such core issues as necessity and proportionality and the very definition of “war” itself - apply to cyberspace.
 - How and can one distinguish between military (combatant) targets and civilian (non-combatant) targets?
 - What would be the implications and what would be the proper range of responses if one nation state were to distribute against another the Stuxnet virus, which attacks SCADA systems that control electrical and power infrastructure?
 - What issues surround use by a nation state of non-governmental proxies, such as bot-net operators, to conduct cyber-attacks?

Economic Concerns

- Economic effects of cyber-crime and cyber-war
- Economic effects of cyber-defense
 - high cost
 - information inefficiencies due to balkanization of networks and databases
- Economic effects of government demands for access to encrypted information
 - Protection of trade secrets
 - Confidential corporate and financial information
 - Confidentiality obligations of lawyers, doctors and accountants

Structuring National Responses

- International cooperation is necessary, but each nation will have to develop, as a foundation, its own national cyber-security capacity. For example:
 - The US Comprehensive National Cyber-security Initiative (CNCI)
 - The European Programme for Critical Infrastructure Protection covering all Member States and the European Economic Area
- Issues for consideration include:
 - What are the most effective means to promote effective coordination and cooperation at the national level?
 - How far should governments go in regulating the private sector in the name of improving cyber-security?
 - What should be the role of civilian agencies versus national security agencies?
 - What should be the roles of law enforcement or national security agencies versus the roles of ministries for trade, commerce or communications

Promoting International Cooperation on Cyber-security

- No nation state can achieve adequate cyber-security on its own; regional and international coordination and cooperation must be part of the response. The Paper lists a variety of activities in this regard:
 - EU and CoE efforts
 - Group 20 meeting in Seoul
 - Efforts at the UN
- International treaty on some or all aspects of the cyber-security problem?
 - What are the key issues that should or could be addressed in a cyber-security treaty?
 - What would be the added value and risks of such a treaty?
 - What incremental steps can be taken to break through the problems?
 - How can treaty compliance be [verified](#)?

Promoting International Cooperation on Cyber-security

- How to reconcile different visions of cyber-security. Some see cyber-security as having state security at its core. Others see Internet governance (including Internet security) as involving an integration and balancing of interests, including national security and human rights and economic and developmental interests
- What are the best venues for improving international cooperation?
- What is the role of intergovernmental organizations, such as the ITU, UNCITRAL or the UN itself?
- What is the role of regional organizations?
- What is the role of the international business community and civil society globally?
- How could countries globally be supported in the strengthening of their cyber-security capacities

Non-state actors and Safe Havens

- Issue: Cyber-crimes that can be considered to rise to a level of use of force that amount cyber-war crimes.
- Not dealing with use of force between or among actors that are clearly state actors.
 - Involves debates over the interplay of Articles 2(4), 51 and 39 of the UN Charter, the concept of “preemptive self-defense” and when cyber-attacks are the equivalent of “kinetic” attacks. These issues are not easily amendable to judicial or other ordinary legal process
- Am dealing with the related problems of non-state actors and “Safe Havens.”
- Non-state actors (or entities disguised a non-state actors) are used as state proxies, such as hackers gangs and botnet operators located on their territories
- Why makes some states provide safe haven to cyber-criminals?

Agreement to ban denial-of-service attacks

- Recent suggestion: Seek an international agreement to **ban denial-of-service attacks** outside conventional conflicts
- Made by US Council on Foreign Relations Council in Special Report No. 56, September 2010 (downloadable gratis at http://www.cfr.org/publication/22832/internet_governance_in_an_age_of_cyber_insecurity.html)

Agreement to ban denial-of-service attacks

- Advantages:
 - Deals with specific problem that is not complicated by intelligence collection.
 - Denial-of-service attacks are, by their nature, brute-force weapons that do not require networks to be penetrated, but only disrupted or sabotaged
 - Provides a good concrete first step to build upon.
 - Most denial-of-service attacks are carried out by criminals for the purpose of extortion
 - The assistance that states provide in shutting down a distributed denial-of-service attacks can be used as a test of whether it is a state act or not
 - Could include attacks on the root

You may download the Background Paper at <http://bit.ly/9xAdAV>

It is also posted under “Committee Documents” on the webpage of the Cyberspace Law Committee of the Section of Business Law of the American Bar Association at

<http://www.abanet.org/dch/committee.cfm?com=CL320000>

It is also posted on the webpage of the Committee’s Task Force on Internet Governance at

<http://www.abanet.org/dch/committee.cfm?com=CL320061>