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.

In this Workshop, we aim to explore the legal aspects of cross-border cyber-security efforts that address the tensions among these conflicting concerns. Selected Bibliographic References are found at Exhibit A.

I. Recent Developments Prompting Heightened Concern

In recent years, cyber-security has become a major concern of governments and the private sector around the world. There seems to have been a major shift in consciousness, stemming from a variety of sources, including:

- Increased appreciation of how critical the Internet and its resources are in multiple spheres of human endeavor and how many infrastructures and systems are increasingly dependent on Internet connectivity and capacity
- Continuing disclosures of major data breaches at financial institutions, other corporations, government agencies and academic institutions globally
- Continuing releases of malware and the increased sophistication of those deployments (e.g., Confiker, Stuxnet and Zeus3 trojan)
- Continuing reports of varying levels of governmental monitoring and filtering (or censorship) of Internet use and content
- The unattributed cyber-attacks on key infrastructure in Lithuania, Estonia, Georgia and other countries
- Concerns with governmental and corporate espionage
Increased concern over cybercrime, including online fraud, identity theft, child pornography, theft of intellectual property, and related criminal money flows on the Internet

Privacy concerns with corporate and governmental data access

As the reach of the Internet continues to scale past a quarter of the world’s population, and given the apparent lack of adequate user awareness on implementation of security protocols, systems operating on the Internet are often perceived as soft targets to a range of entities. These include criminal enterprises, “hackers” (whether for financial gain or as a challenge), cause-based groups, proxies for governments, and governments, including their military and intelligence agencies. Motives for the attacks range from financial gain to the advancement of national security interests to the satisfaction of peer recognition.

II. International, National and Organizational Responses

The global cyber-security problem is multi-faceted and requires a multi-faceted response.

A. Cybercrime – The Law Enforcement Response

In 2001, the Council of Europe (COE) adopted a Convention on Cybercrime. See http://www.conventions.coe.int/cybercrime (the “Budapest Convention”). The treaty addresses three sets of issues: the categories of cybercrime that nations should address in their criminal codes; the authorities governments should adopt in order to access communications or stored records for evidentiary purposes; and mechanisms for transnational cooperation. So far, the Budapest Convention has entered into force in 30 countries, and another 21 countries have signed it or been invited to accede.

At the centennial UN Crime Congress held in April 2010 in Salvador, Brazil, efforts to negotiate a global cybercrime treaty were unsuccessful despite intense discussion among the parties. Disagreements emerged over national sovereignty issues and concerns for human rights, among other issues.

Questions for consideration include how these disagreements can be bridged, the need to balance different interests and rights, including security and privacy as well as the impact of rapidly developing technologies on the structure of any agreement. For instance, the current review of the Council of Europe Data Protection Convention is exploring new ways for addressing concerns related to privacy protection and security in the context of trans-border data flow taking into account constantly emerging information and communication technologies.

Other regional or international bodies have put forth models or recommendations for national cybercrime legislation, based on the Budapest convention. For example, the Commonwealth of Nations has issued a “Model Law on Computer and Computer Related Crimes,” http://www.thecommonwealth.org/shared.asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. Moreover, according to the COE, some 100 countries have made use of the Budapest Convention when developing national cybercrime legislation. Likewise, the International Telecommunications Union has developed draft cybercrime legislation, which can be found at http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.
Cybercrime raises many traditional law enforcement issues. A recent dispute between the US and the UK, for example, illustrates how traditional tensions over extradition also arise in the cybercrime context. See http://www.guardian.co.uk/world/2010/jul/21/gary-mckinnon-extradition-david-cameron. While local limitations of resources and expertise present hurdles to effective law enforcement, one of the trans-national barriers of a legal nature that should be considered is the existence of nation states that serve as “safe havens” and what dynamics and incentives are involved for a nation state to maintain “safe haven status.”

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

Much of the critical infrastructure that is dependent upon information and communications technologies is owned and operated by the private sector; this is true of the Internet itself and the telecommunications networks over which it operates. Other critical infrastructure is owned by governmental or quasi-governmental entities, and there is extensive connectivity between private and governmental networks.

All three elements (private sector, governmental sector and the major linkages between them) can be better protected both by making them more secure, in order to prevent improper access, and by effectively responding to attacks after the fact.

The private sector, on a national and international basis, has been taking steps to increase the security of its products, services and networks. These efforts include, for example, the work of international standards bodies, which range from the treaty-based ITU to non-governmental but highly influential and essential bodies such as the Internet Engineering Task Force (IETF). Important issues for consideration include the role of standards and the role of government in developing standards.

Although the rate of adoption has not been as rapid as one might ideally want, ICANN’s successful effort to promote development and adoption of security extensions for the domain name system (DNSSEC) illustrates how a private-sector led initiative (with government participation) can significantly enhance cyber-security. See http://www.dnssec.net. See also ENISA’s Good Practices Guide for Deploying DNSSEC at http://www.enisa.europa.eu/act/res/technologies/tech/gpgdnssec.

Many governments, often in cooperation with commercial enterprises and educational institutions, have created entities that help government agencies and the private sector respond to and defend against cyber-attacks and identify and correct cyber-vulnerabilities. These are often known as Computer Emergency Response Teams (CERTs). Among other functions, they are intended to promote information sharing and better coordination among government agencies and the private sector. The Forum of Incident Response and Security Teams (http://www.first.org) is an international NGO that seeks to promote global cooperation and coordination among these teams. Its membership includes over 200 teams across 28 countries.

The European Government CERTs (EGC) Group (http://www.egc-group.org) has 11 member organizations. The primary objective of EGC is to develop efficient and effective cooperation between the teams with a focus on incident and vulnerability management. Primarily, EGC is an operational group with a technical focus; national policy is determined by other agencies within individual countries.
C. Cyber-War – The Military and Diplomatic Response

In January 2010, ITU Secretary General Hamadoun Toure proposed at the World Economic Forum in Davos that the world’s nations should adopt a treaty in which they would engage not to make the first cyber strike against another nation. The ensuing debate revealed a considerable lack of clarity over what cyber-war is and what responses are appropriate for nation states to exercise. The fundamental issue is how does the “law of war” – including such core issues as necessity and proportionality and the very definition of “war” itself - apply to cyberspace. For example, assuming that use of force was otherwise justified, when would it be appropriate to attack the systems (SCADA) that control electrical and power infrastructure, and would it be necessary or even possible to 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? What issues surround use by a nation state of non-governmental proxies, such as bot-net operators, to conduct cyber-attacks?

These issues are arising in a variety of forums. Recently, for example, NATO issued an experts report, “NATO 2020: Analysis and recommendations of the group of experts on a new strategic concept for NATO” http://www.nato.int/strategic-concept/expertsreport.pdf, which 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 provides that “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. See Internet War Crimes Tribunals and Security in an Interconnected World, Sharon R. Stevens at http://www.uiowa.edu/~tlcp/TLCP%20Articles/18-3/stevens.finalfinal.me.mlb.100109.pdf; Cyberwar and customary international law: the potential of a "bottom-up" approach to an international law of information operations, Jon P. Jurich, 9 Chi. J. Int'l L. 275-295 (2008); Influencing and Exploiting Behavioral Norms in Cyberspace to Promote Ethical and Moral Conduct of Cyberwarfare, Lt. Col. Glen R. Shilland, at https://www.afresearch.org/skins/rims/q_mod_be0e99f3-fc56-4ccb-8def-670c0822a153/q_act_downloadpaper/q_obj_4112703c-47be-4d4d-93c2-8276ab2f35a3/display.aspx?rs=enginespage.

D. Structuring National Responses

While international cooperation is necessary, each nation will have to develop, as a foundation, its own national cyber-security strategy, authorities and capabilities. Within any given nation state, adequate cyber-security will require effective coordination and cooperation among governmental entities on the national and sub-national levels as well as the private sector and civil society.

Issues for consideration include: What are the most effective means to promote effective coordination and cooperation at the national level? To what extent should cooperation of the private sector be legally compelled? What incentives or subsidies may promote cooperation? How far should governments go in regulating the private sector in the name of improving cyber-security? What is the role of civil liability systems in addressing cyber-vulnerabilities?
As governments seek to develop their own national policies and structures for cyber-security, questions include which agency or ministry should have the lead? 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?

One example of a national strategy for cyber-security is the Comprehensive National Cybersecurity Initiative (CNCI) developed by the US. See http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative It is important to note that most elements of the US plan focus on getting the federal government’s own cyber-security house in order. The US has not decided what should be the regulatory authority of the federal government in protecting critical infrastructures owned and operated by the private sector. Pending legislation may clarify that role later this year.


One element of almost any cyber-security strategy at the governmental or corporate level is the development and deployment of intrusion detection systems that monitor a given network for unauthorized traffic and malicious content. Key issues include whether an intrusion detection system for governmental networks should be extended to privately owned networks or should the private sector manage its own intrusion detection systems? If the answer in a particular nation is that an intrusion detection system for governmental networks should be extended to at least some more critical privately owned networks, the next question is on what principles is that category delineated. This issue also often leads to consideration of the role of national security or military agencies versus civilian agencies.

E. Economic Concerns

Cybercrime and cyber-war have obvious direct negative effects on economic activity and in fact may be intended do so in the case of cyber-war. Cyber-defense can have similar direct negative effects, if only due its high cost and the information inefficiencies due to deliberate isolation of networks and databases from one another. There are, however, a number of situations in which information security has less obvious negative effects that reflect the tensions that are the subject of this paper. For example, recent developments involving RIM’s Blackberry service and demands by the UAE, Saudi Arabia and India have uncertain effects on the ability of business and various professional such as lawyers, doctors and accountants to meet their legal obligations regarding trade secrets and confidential business information. See http://www.nytimes.com/2010/08/18/business/global/18rim.html?_r=1&ref=research-in-motion-ltd and http://www.nytimes.com/2010/08/11/technology/11rim.html?ref=research-in-motion-ltd.

F. Promoting International Cooperation on Cyber-security

No nation state can achieve adequate cyber-security on its own; international coordination and cooperation must be part of the response.

Some believe that an international treaty is needed on some or all aspects of the cyber-security problem. Questions for consideration include: What are the key issues that should or could be
addressed in a cyber-security treaty? What would be the added value of such a treaty? What would be the risks? What prior efforts have been attempted and what caused them to fail or have limited effect? What incremental steps can be taken to break through the problems? How can treaty compliance be verified? How could countries globally be supported in the strengthening of their cyber-security capacities, through technical assistance and other means?

Any effort to reach international consensus on cyber-security is likely to expose a range of concerns, which in part flow from different visions of national security, of the role and value of the Internet, of human rights, and of economic policy. Some see cyber-security as having state security at its core, which leads to an emphasis on capabilities to monitor and attribute transmissions and to block any undesirable content. Others strongly believe that Internet governance (including Internet security) involves an integration and balancing of interests, including not only national security but also human rights and the economic and developmental interests associated with a vibrant, innovative and competitive ICT sector. These differing perspectives manifest themselves in many areas, including, for example, the increasing debate over the issue “attribution,” referred to above. One contribution to reconciling these interests is the 2009 recommendation of the European Parliament on strengthening security and fundamental freedoms on the Internet.


Various proposals are emerging for improving regional and international cooperation.

The Council of Europe has started work to explore the shared responsibilities of states to take reasonable measures through multi-lateral cooperation to ensure the ongoing functioning of the Internet and, in consequence, the delivery of the public service to which all persons under their jurisdiction are entitled. See Resolution Internet Governance and critical Internet resources adopted at the 1st Council of Europe Conference of Ministers responsible for Media and New Communication Services, 28-29 May 2009, Reykjavik at http://www.coe.int/t/dghl/standardsetting/media/MCM%282009%29011_en_final_web.pdf (at pg.9).

In this connection, the competent intergovernmental cooperation body, the COE Steering Committee on the Media and New Communication Services (CDMC), has been asked by the COE Committee of Ministers to give priority attention to the elaboration of legal instruments designed (i) to preserve or reinforce the protection of the cross-border flow of Internet traffic and (ii) to protect resources which are critical for the ongoing functioning and borderless nature and integrity of the Internet (i.e. critical internet resources).

It was reported recently that Korea is attempting to present computer security as a topic of discussion for the Group of 20 meetings in Seoul later this year. Korea reportedly wants to include on the summit agenda discussion of establishing an international body for combating cybercrime. See http://www.infowar-monitor.net/2010/08/korea-trying-to-put-cybersecurity-on-g20-agenda/

In March 2009, the EU Commission issued a communication on Critical Information Infrastructure Protection (CIIP), entitled “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience” See http://ec.europa.eu/information_society/policy/nis/docs/comm_ciip/comm_en.pdf. It noted that the challenges for Europe are: (1) Uneven and uncoordinated national approaches; (2) need for
a new European governance model for Critical Information Infrastructures; (3) limited European early warning and incident response capability; and (4) need for appropriate international cooperation. With respect to international cooperation, the communication spoke of “….engaging the global community to develop a set of principles, reflecting European core values, for Internet resilience and stability, in the framework of our strategic dialogue and cooperation with third countries and international organisations.”


One structure in Europe for improving coordination is the European Network and Information Security Agency (ENISA), founded in 2004. ENISA is planning the first pan-European CIPP exercise to take place in November 2010. The exercise will test the efficiency of communication between different Member States in case of incidents affecting Internet’s normal operation in all participating countries.


Issues for consideration include 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, such as the African Union, APEC, the Council of Europe, the EU, NATO or the OAS? What is the role of the international business community and civil society globally? What incremental steps can be taken to advance cooperation?
Exhibit A

Selected Bibliographic References


Baker, Stewart (2010) Skating on Stilts


Charney, Scott, *Rethinking the Cyber Threat A Framework and Path Forward*, 


Cohen, Julie E. 2003, *DRM and Privacy:*
http://www.law.berkeley.edu/journals/btlj/articles/vol18/Cohen.stripped.pdf


*CSIRT Services.* http://www.cert.org/csisrts/services.html

*Cyber Security: A New Model for Protecting the Network* – The World Bank Group, Global ICT Department

This Background Paper has been drafted to meet an IGF requirement for Workshops feeding into main sessions and reflects contributions by Henry Judy, Jim Dempsey, David Satola, and Lee Hibbard in their individual capacities. It does not necessarily reflect the views (official or unofficial) of any organizations with which they are respectively associated, nor of any personnel of any organizations participating in this Workshop.


This Background Paper has been drafted to meet an IGF requirement for Workshops feeding into main sessions and reflects contributions by Henry Judy, Jim Dempsey, David Satola, and Lee Hibbard in their individual capacities. It does not necessarily reflect the views (official or unofficial) of any organizations with which they are respectively associated, nor of any personnel of any organizations participating in this Workshop.


In general, refer to the following comprehensive website:

http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm


Knake, Robert K., July 2010. Untangling Attribution: Moving to Accountability in Cyberspace, Prepared Statement Before the Subcommittee on Technology and Innovation, Committee on
Science and Technology, United States House of Representatives 2nd Session, 111th Congress


Ponemon Institute Study Shows Lack of Accountability, Resources at Root of U.S. Corporate Data Loss Problem, August 28, 2006.

http://www.ponemon.org/press/Ponemon_Port_AuthorityDetectPr.pdf


http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project/567-d-3progrep1PROV-Public_11aug08_en.pdf


Raul, Alan Charles and Ed McNicholas, October 2007. Defendant Prevails in Privacy Case where Data Theft Results in No Injury to Plaintiffs, Privacy & Data Security Law Journal


Reichman, J.H. and Paul F. Uhlir, 1999. Database Protection at the Crossroads: Recent Developments and Their Impact on Science and Technology
This Background Paper has been drafted to meet an IGF requirement for Workshops feeding into main sessions and reflects contributions by Henry Judy, Jim Dempsey, David Satola, and Lee Hibbard in their individual capacities. It does not necessarily reflect the views (official or unofficial) of any organizations with which they are respectively associated, nor of any personnel of any organizations participating in this Workshop.

http://www.law.berkeley.edu/journals/btlj/articles/vol14/Reichman/html/reader.html


http://www.law.berkeley.edu/journals/btlj/articles/vol18/Skibell.web.pdf

Replies on Mutual Legal Assistance in Computer-Related Cases – European Committee on Crime Problems (CDPC) and the Committee of Experts on the Operation of European Conventions on Co-operation in Criminal Matters (PC-OC) – Strasbourg, 1 December 2008.

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/PC-OC%202008-%202008%20Rev%20Computer%20Related%20cases.pdf

Resources for Computer Security Incident Response Teams (CSIRTs).

http://www.cert.org/csirts/resources.html


http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf


http://groups.ischool.berkeley.edu/samuelsonclinic/files/cso_study.pdf
This Background Paper has been drafted to meet an IGF requirement for Workshops feeding into main sessions and reflects contributions by Henry Judy, Jim Dempsey, David Satola, and Lee Hibbard in their individual capacities. It does not necessarily reflect the views (official or unofficial) of any organizations with which they are respectively associated, nor of any personnel of any organizations participating in this Workshop.

Staffing Your Computer Security Incident Response Team – What Basic Skills Are Needed?
http://www.cert.org/csirts/csirt-staffing.html

Summary – Global Project on Cybercrime (Phase 2) – Version 20 February 2009.
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project/2079%20admin%20pro%20summary1a%20%20Feb%202009.pdf


The Commonwealth -- Model Law titled: “Computer and Computer Related Crimes Bill – available online at:

The E-Government Handbook for Developing Countries – November 2002 – A project of infoDev and The Center for Democracy & Technology


http://www.whitehouse.gov/the_press_office/AdvisorsToConductImmediateCyberSecurityReview/


http://works.bepress.com/cgi/viewcontent.cgi?article=1011&context=joseph_turrow


http://www.cert.org/csirts/resources.html
This Background Paper has been drafted to meet an IGF requirement for Workshops feeding into main sessions and reflects contributions by Henry Judy, Jim Dempsey, David Satola, and Lee Hibbard in their individual capacities. It does not necessarily reflect the views (official or unofficial) of any organizations with which they are respectively associated, nor of any personnel of any organizations participating in this Workshop.