International Cybersecurity Legal Frameworks and Internet Governance

University of Maryland Baltimore Campus
Cybersecurity Graduate Program
October 17, 2011

Henry L. Judy
K&L Gates LLP
1601 K Street, NW
Washington, DC 20006-1600
(202) 778-9032
henry.judy@klgates.com
http://www.klgates.com

Some Organizational Background

- American Bar Association
  - Section of Business Law
    - Cyberspace Law Committee http://apps.americanbar.org/dch/committee.cfm?com=CL320000
    - Task Force on Internet Governance
      - (HLJ and David Satola = Co-Chairs (dsatola@worldbank.org) http://apps.americanbar.org/dch/committee.cfm?com=CL320061
    - Additional resources on TF webpage, *e.g.,*
      - Task Force Presentation at Oxford Internet Institute
      - Corporate Governance as Internet Governance: A Corporate Law and Operational Analysis Of Key ICANN Functions (Draft - 11/09)
  - Mission of TF is:
    - Educational for the bar as whole and the business law bar especially
    - Help bar see over the horizon; not just immediate issues

Some Organization Background

- United Nations
  - Internet Governance Forum http://www.intgovforum.org/cms/
    - Annual Meetings
      - 2011 Nairobi, Kenya
      - 2010 Vilnius, Lithuania
      - 2009 Sharm El Sheikh
      - 2008 Hyderabad, India
      - 2007 Rio de Janeiro, Brazil
      - 2006 Athens, Greece

Some Organization Background

- Managed by a Secretariat in Geneva, Switzerland
- Advised by a “Multi-stakeholder Advisory Group” (MAG).
- IGF operates on Multi-stakeholder Model
  - Multi-stakeholder governance” (“MSG”) or the “multi-stakeholder model” may be described as a more “bottoms-up” approach, in which governments, private companies, civil society, the technical community and other independent organizations all have roles to play but in which no single entity operates without checks and balances
  - The model is more directly representative and at the same time gives rise to tensions among the various parties, as they seek to enhance relative positions of influence
  - Contrast to “Governments Only” or “top-down” model
- ABA as “civil society” participant organizes “workshops” and otherwise generally participates

Plan A for this Discussion

- First Part
  - Workshop Paper in Vilnius → Law Review Article in William Mitchell Law Review
  - Focuses on International Cybersecurity Legal Frameworks
  - PDF of Law Review article available from Prof. Thompson
- Second Part
  - Presentation at ABA Annual Meeting in Toronto in August 2011 → law review article in 2012 in the Law Review of the Chase College of Law at Northern Kentucky University
  - Focuses on theory of Internet Governance
- Concept is to move from more particular to the more general
- Also, in this discussion, put out a lot of data and issues and periodically tie them up

Workshop Theme in Vilnius

- 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

Outline – Vilnius Background Paper and Discussion

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. Protecting Economic Interests

E. Structuring National Responses

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 at financial institutions, other corporations, government agencies, and academic institutions globally
- Continuing releases of more sophisticated malware
- Continuing reports of varying levels of governmental monitoring and filtering (or censorship) of Internet use and content
- Cyber-attacks on key infrastructure in various countries and on the databases of major global business corporations
- Concerns with governmental and corporate espionage
- Increased concern over cyber-crime online fraud, identity theft, child pornography, theft of intellectual property 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/data protection 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

Council of Europe (CoE)

- Before moving to networks -----
- CoE http://www.coe.int/lportal/web/coe-portal/home
  - international organization promoting co-operation the areas of legal standards, human rights, democratic development, the rule of law and cultural co-operation
  - 47 member states (EU and non-EU); cannot make binding laws
  - However, currently 210 conventions and other treaties (http://www.conventions.coe.int/Treaty/Commun/ListeTraites.asp?CM=8&CL=ENG) which other countries can sign, ratify and cause to enter into force
  - Convention on Cybercrime (Budapest Convention - 2001) http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=16/10/2011&CL=ENG

Data Protection

- Data Protection
  - US law -- “privacy” and “information security” commonly referred to separately although they two side of the same coin
  - EU law – “data protection” (more precisely, “personal data protection”) means both
  - Both systems of law use “Personally Identifiable Information’ (or “PII”)
  - To the extent both systems more strictly protect PII, the level of cybersecurity is enhanced
    - Simple example: If holders of PII are require to delete or anonymize it sooner, infosec is increased because you can’t steal what doesn’t exist or that which is no longer PII
  - The two systems are in fact becoming more strict and they are gradually converging

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.
- United Nations Charter
  - Article 2(4) - "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."
  - Article 39 – "The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security."

Cyber-War – The Military and Diplomatic Response

- Article 41 – “The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures.”
- Article 42 – “Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations
- Article 51 - “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 interplay of these and related Articles of the UN Charter, the concept of “preemptive self-defense” and when cyber-attacks are the equivalent of “kinetic” attacks have been hotly debated. These issues are not easily amendable to judicial or other ordinary legal process.
- How does the “law of war” – including such core issues as legitimacy, necessity and proportionality and the very definition of “war” itself - apply to cyberspace. For example,

Cyber-War – The Military and Diplomatic Response

- 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?

- Cyber-crimes that can be considered to rise to a level of use of force that amount cyber-war crimes, *e.g.*, massive theft
- How does one and can one distinguish between or among actors that are clearly state actors and non-state actor?
- 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
- What makes some states provide safe haven to cyber-criminals?

Protection of Economic interests

- 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

Recent Attack Examples

- Operation Aurora (2009)
  - cyber attack which began in mid-2009 and continued through December 2009
  - Targets Google, Adobe Systems, Juniper Networks, Rackspace, Yahoo, Symantec, Northrop Grumman, Morgan Stanley and Dow Chemical
- Operation Shady Rat (2011)
  - Targets included US, Canada, and South Korea governments, the UN, the International Olympic Committee, and 12 US defense contractors Targets were found in 14 different countries, across North America, Europe, India, and East Asia.
  - Named after remote administration tools (or "RATs) that are installed in the targeted organization
- Similar to spear-phishing attacks on Lockheed Martin, security-device maker RSA, treasuries of Britain and France, the IMF, Canadian defense ministry, EU Commission, EU Parliament, Australian parliament, Citigroup, and Department of Energy's Oak Ridge National Lab

Recent Attack Examples

- Operation Black Tulip (2011)
  - Involves compromise of Dutch Certificate Authority DigiNotar
  - Domains for which fraudulent certificates were issued includes Facebook, Google, Microsoft, Yahoo!, Tor, Skype, Mossad, CIA, MI6, LogMeIn, Twitter, Mozilla, AOL and WordPress.
  - See full list of compromised certificates at https://blog.torproject.org/blog/diginotar-damage-disclosure
  - Report of security auditors, Fox IT, at http://www.rijksoverheid.nl/ministeries/bzk/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html
- Note: The motivation for these attacks is not embarrassment (Anonymous, Wikileaks) or the lulz (LulzSec). They are done to damage major infrastructure and cause severe economic loss

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

Some Personal Views

- The most fundamental problem with a Top-Down approach to international legal structures for cybersecurity is a conflict of values. Accepting the CoE convention, for example, means accepting:
  - That security, including infosec, means primarily protecting citizens and private interests rather than protecting the State and the party that controls it
  - The rule of law – the primacy of non-arbitrary processes
  - The jurisdiction of institutions not under the control of the State and the party that controls it

Some Personal Views

- Safe Havens
  - Lack of capacity
  - Money
  - Useful as bases for deniable (but controllable) proxies
- Issues in democracies
  - Relative roles of state in providing security
  - Access to personal data
- No choice
  - Defense is hard and expensive, but offense is more dangerous
  - Bottom-up MSG may be messy and gradual, but the adverse consequences of top-down are worse

Second Part

- Have prepared draft paper titled “Internet Governance: Global Developments Systematically Considered”
- Paper presents the process and development of Internet Governance as a system of inter-connected issue areas
- Follows up on previous article in William Mitchell Law Review
- This presentation summarizes the current version of the paper
- Used the paper at the IGF in Nairobi in September 2011
- Will be published in the Law Review of the Chase College of Law at Northern Kentucky University

Remember this Definition?

- “Multi-stakeholder governance” (“MSG”) or the “multi-stakeholder model” may be described as a more “bottoms-up” approach to Internet Governance, in which governments, private companies, civil society, the technical community and other independent organizations all have roles to play but in which no single entity operates without checks and balances
- It is not just a model for running conducting the IGF; it is considered a model for governing the Internet
- The model is more directly representative and at the same time gives rise to tensions among the various parties, as they seek to enhance relative positions of influence

Perception: Change in Awareness

- Nature and situs of Internet Governance agenda has changed, moving up and to the center of the international policy:
  - Shift away from being largely technical
  - Shift away from focus on ICANN
    - "Legacy" tensions about governmental "control" remain
  - IG issues are now better understood, emotional temperature has dropped
  - Skepticism about workability and advantages of "MSG" model largely overcome; however, continuing major resistance to the concept by a number of major governments
  - IG debate – formerly the province of Telco Ministries and specialized NGOs - is now the subject public comments by Secretaries of State, Presidents of major nations, and senior military and business leaders

Substance: IG Direction and Domains

- Today, there is no “top down” Internet governance (or formation of international legal structures for dealing with cybersecurity)
- However, past year has witnessed a shift from focus on “institutions” and “roles”, to focus on issue areas we shall call “domains”
- Internet Governance” is more the net effect at any given time of actions and actors across these “domains”
- Domains are tightly linked conceptually and operationally…actions in any one domain affect other domains
- Consistent with “multi-stakeholder” approach to IG
- Our focus is on legal and related policy domains; full theory would include technical and developmental domains

Domains

- The paper considers the following Domains
  - Domain of Global Intergovernmental Action
  - Domain of Non-Governmental Organizations
  - Human Rights Domain
  - Intellectual Property (IP) Domain
  - Privacy and Data Protection Domain
  - Information Security Domain
  - Telecommunications Policy Domain
  - Military Domain
  - Jurisdiction Domain

Current Predominant Domains

- Each of the individual domains may also be thought of as a vector, and the state of Internet Governance at any point in time may be thought of as the net vector that is the cumulative result of the individual vectors. (Pick your metaphor)
- In our view, the predominant vectors or domains currently the domains of Human Rights and Information Security

Domain of Global Intergovernmental Action ".igo"

- US International Strategy for Cyberspace (May 2011)
  - "Upholding Fundamental Freedoms: States must respect fundamental freedoms of expression and association, online as well as off."
    - Human Rights Domain is lead "Norm" in Strategy
  - "Multi-stakeholder Governance: Internet governance efforts must not be limited to governments, but should include all appropriate stakeholders." "(MSG)"
- Organisation for Economic Co-operation and Development (OECD) Meeting (June 2011)
  - Communiqué favoring MSG

Domain of Global Intergovernmental Action ".igo" cont.

- 2011 G-8 Summit (May 2011)
  - Comprehensive Declaration echoing US International Strategy
- The e-G8 Forum
  - Informal Forum if Internet executives organized by France
  - No formal positions but sharply laissez-faire mood
- International Telecommunications Union (ITU)
  - Plans to seek some top-down authority at ITU's World Conference on International Telecommunications (WCIT) in 2012
  - General resists MSG; favors top-down IG in governments using ITU as their agent

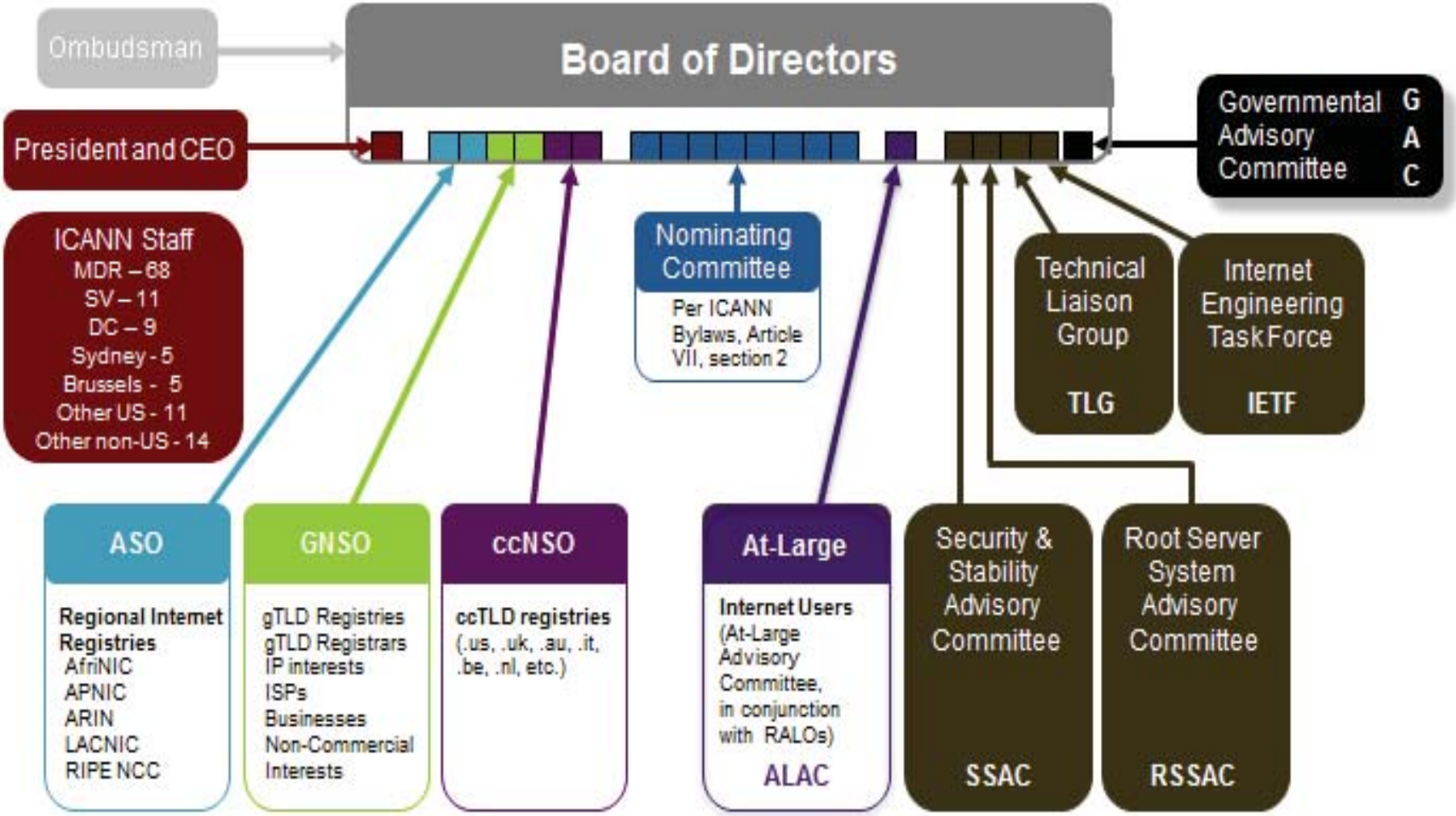
Domain of Global Intergovernmental Action ".igo" cont

- China and Russia are leading opponents of MSG
  - Favor government-only IG
  - Favor major UN role in international IG and specifically the ITU
- Chinese Developments
  - China very forward in articulating views on IG
  - Views available in English
  - China actively implementing its views within its borders
  - White Paper on the Internet (June 2010)
  - Comprehensive state regulation within its borders
  - Favors international agreement on content regulation

Domain of Non-Governmental Organizations ".ngo"

- Internet Corporation for Assigned Names and Numbers (ICANN) http://www.icann.org/
  - ICANN favors MSG and is explicitly structured on that model (see next slide)
  - However, top-down vs. MSG tension played out in tensions between the Governmental Advisory Committee (GAC) and Board and Staff
    - Accountability and Review Team Report & Implementation
    - .xxx gTLD ("dot triple x") approval
    - gTLD expansion (www.office.microsoft, instead of www.office.microsoft.com) discussed under IP Domain below
  - Currently playing out in context of renewal of the contract with Internet Assigned Numbers Authority (IANA)

ICANN Multi-Stakeholder Model



Domain of Non-Governmental Organizations ".ngo"

- Internet Governance Forum (IGF)
  - Already discussed
  - Co-chair D. Satola participated in Nairobi Forum
- The Internet Society
  - Strong support for MSG
- Other NGOs

Human Rights Domain ".hr"

Art. 19 of the International Covenant on Civil and Political Rights provides that:
"Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."

"The exercise of the rights provided for in paragraph [above] of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; [and] (b) For the protection of national security or of public order (ordre public), or of public health or morals."

Human Rights Domain ".hr"

- United Nations
  - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression
- When a restriction is imposed as an exceptional measure on online content, it must pass a three-part, cumulative test:
  - it must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency);
  - it must pursue one of the purposes set out in article 19, paragraph 3, of the International Covenant on Civil and Political Rights, (principle of legitimacy); namely:

Human Rights Domain ".hr"

- to protect the rights or reputations of others;
- to protect national security or public order, or public health or morals, and
- it must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality).

- In addition, any legislation restricting the right to freedom of expression must be applied by a body which is independent of any political, commercial, or other unwarranted influences in a manner that is neither arbitrary nor discriminatory (principle of independence)
- There should also be adequate safeguards against abuse, including the possibility of challenge and remedy against its abusive application.

Human Rights Domain ".hr"

- Council of Europe
  - On September 23, 2011 CoE announced the adoption by its Committee of Ministers of two recommendations and two declarations calling, *inter alia*, on CoE member states to take action to protect on-line freedom of speech, even in the face of national security responses to cyber threats. Declaration of Internet Governance Principles linked net neutrality and human rights. While avoiding the term "net neutrality," Principle 9, entitled "Open Network" provides:
  - *"Users should have the greatest possible access to Internet-based content, applications and services of their choice, whether or not they are offered free of charge, using suitable devices of their choice. Traffic management measures which have an impact on the enjoyment of fundamental rights and freedoms, in particular the right to freedom of expression and to impart and receive information regardless of frontiers, as well as the right to respect for private life, must meet the requirements of international law on the protection of freedom of expression and access to information, and the right to respect for private life. "*
  - https://wcd.coe.int/wcd/ViewDoc.jsp?Ref=DC-PR079(2011)&Language=lanEnglish&Ver=original&Site=COE&BackColorInternet=F5CA75&BackColorIntranet=F5CA75&BackColorLogged=A9BACE

Human Rights Domain ".hr"

- Expanding Means of Censorship
  - Mandatory routing through government controlled servers
  - Government-sponsored (required) email service
  - Dual Internet
    - Cuba
    - North Korea
    - Iran (in development)

IP Domain ".kaos"

- Information security failures are a leading cause of loss of IP protections
- gTLD Expansion
  - New (June 2011) ICANN program it is possible for organizations (entities, not individuals) to reserve new generic Top-Level Domain names (gTLDs)
  - Potentially one of biggest changes ever to the Internet's Domain Name System. Subject to restrictions in the program, Internet address names will be able to end with almost any word in any language.
  - Topic discussed under IP heading because protection of trademarks and loss of trademark protection was key battlefield.
    - However, top-down governmental control over culture was equally key. For example, www.abc.Jesus
  - Applications for new gTLDs will be accepted from 12 January 2012 to 12 April 2012

IP Domain ".kaos"

- "An applicant for a new gTLD is, in fact, applying to create and operate a registry business supporting the Internet's domain name system." http://newgtlds.icann.org/applicants/faqs
- gTLD expansion is complicated by ICANN's development of the Internationalized Domain Names (IDNs) system. These are domain names represented by local language characters, including letters or characters from non-ASCII scripts.
  - For example, on the country code level, rather than .ru, the IDN ccTLD .рф (Cyrillic for **Р**оссийская **Ф**едерация, **R**ussian **F**ederation) is open for general registration

IP Domain ".kaos"

- Anti-Counterfeiting Trade Agreement
  - Targets intellectual property piracy
  - Recently signed by US, Australia, Canada, Japan, Morocco, New Zealand, Singapore and South Korea. EU, Mexico and Switzerland did not sign but "confirmed their continuing strong support for and preparations to sign the agreement as soon as practical"
  - Requires governments make it unlawful to market devices that circumvent copyright, such as devices that copy encrypted DVDs without authorization.
  - Analogous to US Digital Millennium Copyright Act in the US
  - Calls on participating nations to maintain extensive seizure and forfeiture laws when it comes to counterfeited goods that are trademarked or copyrighted
  - Participating nations must implement a legal system whereby victims of intellectual property theft may be awarded monetary damages.

Privacy and Data Protection Domain ".prv"

- Previously discussed
- However, want to emphasize that:
  - Right to privacy is treated as a key right under general human rights principles
  - Information security failures are a leading cause of loss of privacy protections

Information Security Domain ".infosec"

- US National Cyber-Security Plan
  - White House sends legislative plans to Congress (May 2011)
  - Mixed reception
- DOD Actions
  - Creation of Cyber Command
- Department of Homeland Security
  - Published a new system of guidance intended to help make the software behind Web sites, power grids and other services less susceptible to hacking. Includes an updated list of the top 25 programming errors that enable today's most serious hacks (June 2011)

Information Security Domain ".infosec"

- Securities and Exchange Commission
  - On October 13, 2011 the SEC's Division of Corporation Finance issued "CF Disclosure Guidance: Topic No. 2" providing that Division's views regarding disclosure obligations relating to cybersecurity risks and cyber incidents. http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
  - Based on concept that companies report must "material" developments, or matters significant enough that the average investor would want to know about them
  - Key points
    - Supplements absence of Federal breach notice requirement (other than for financial institutions)
    - How meaningful is boiler-plate disclosure? Everybody is a risk and hacking attempts on public companies are made daily (hourly)
    - Further SEC guidance will become key part of global dialog

Telecommunications Policy Domain
".telco"

- Net neutrality
  - Two sides on the international stage:
    - issue is mainly a technical matter (*e.g.*, reasonable traffic management, applicability to what services and antitrust)

      versus
    - issue is mainly respect for fundamental rights, such as freedom of expression, freedom to conduct business and data protection
  - Example: Proposed CoE net-neutrality recommendation:
    - any traffic management measure or privilege should be nondiscriminatory, justified by overriding public interest, and must meet the requirements of international law on the protection of freedom of expression and access to information."

Telecommunications Policy Domain ".telco"

- Example:
  - Opinion of the European Data Protection Supervisor "on net neutrality, traffic management and the protection of privacy and personal data" (October 7, 2011)
  - "Net neutrality refers to the issue of whether Internet service providers (ISPs) should be allowed to monitor network traffic to filter or restrict Internet access, for example to block specific services or applications (e.g. peer to peer) or give preference access to others. …Certain inspection techniques used by ISPs may indeed be highly privacy-intrusive, especially when they reveal the content of individuals' Internet communications, including emails sent or received, websites visited and files downloaded." http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/News

Military Domain ".war"

- US Department of Defense Strategy for Operating In Cyberspace (published July 14, 2011)
  - Outlines how DoD will protect its networks and those of its military contractors from cyber-attacks.
  - Strategy envisages that the US will move over time from current emphasis on defense to "deterrence," by which it means a willingness to retaliate with its own virtual weapons and/or military force
  - Note that HR principles of legitimacy, necessity, proportionality are analogously applicable here

Jurisdiction Domain ".jur"

- Cutting across all of the domains is the issue of legal jurisdiction. Some particular challenges:
  - Proliferation of data centers whose architecture makes them "geo-independent"
  - Binding Corporate Rules under EU data protection law
  - "Safe havens"
  - Professional licensing

A Legal Paradigm

- Consider the generality of this legal paradigm:
  - Rule
    - Exception(s) (aka, derogation(s))
      - Rules of interpretation
- Example
  - No war w/o UN Security Council Approval
    - But, Individual or collective self-defense
      - Legitimacy, necessity, proportionality
- Example
  - No restriction on access to info or content of info
    - But, *Ordre public*
      - Predictability, transparency, legitimacy, necessity, proportionality, independence

A Legal Paradigm

- Example
  - No collection of “sensitive personal data”
    - But, Explicit consent, good of subject, *Ordre public*
      - Predictability, transparency, legitimacy, necessity, proportionality, independence
- Specific Example
  - No shut down of cell phone service by government
    - But SF BART (a government agency), citing safety reasons (*ordre public*), shuts down underground service to thwart coordination of anticipated protest in a station over alleged BART Police brutality
      - Legitimacy (permissible under FCC Act or rules?); necessity (protest never happened); proportional (?)
  - Is the analysis different if the wireless service is offered by a private institutions - cafe, hotel, university, etc.?

Use the paradigm to analyze

- On September 12, 2011 China, the Russian Federation, Tajikistan and Uzbekistan released a Resolution for the UN General Assembly entitled "International code of conduct for information security." http://blog.internetgovernance.org/pdf/UN-infosec-code.pdf
- The "code" states, inter alia:
  - "Reaffirming that policy authority for Internet-related public issues is the sovereign right of States"
  - "To cooperate ….in curbing the dissemination of information that incites terrorism, secessionism or extremism" or that "undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment"
  - "To reaffirm all the rights and responsibilities of States to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack and sabotage"
  - "To fully respect rights and freedom in information space, including rights and freedom to search for, acquire and disseminate information on the premise of complying with relevant national laws and regulations"
  - "To promote the establishment of a multilateral, transparent and democratic international Internet management system to ensure an equitable distribution of [Internet] resources …"

Conclusions

- Impact of globalization on formerly tightly bounded concept of the traditional nation state
- Leads to need for increased capacity among regional and international structures to mediate interactions
- By what principles will those interactions be mediated? Suggest that the multi-stakeholder model should be the general model for IG and more broadly
- Avoids a fundamental problem with top-down direction from essentially government actors
  - Any intergovernmental organization that is authorized to hold top-down authority either is likely to unable to agree on the application of the central and pervasive domain of human rights law or is likely to make unacceptable compromises in the same domain. The choice is between unacceptable alternatives of ineffectiveness and loss of individual rights.
- The multi-stakeholder model works and its consistent with and fosters our essential humanity

Conclusions

- While “future scenarios” of IG evolution are difficult to predict, given the highly dynamic inter-relationship of the “domains,”
  - Keep abreast of and be adept at giving ***advice about the impact of, and inter-relationships among, different “domains”*** particularly
    - ***at the international level*** (*e.g.,* human rights) that may be ***outside traditional comfort zone***; or
    - that rely on ***specialized areas*** (*e.g.,* competition, privacy, intellectual property, conflict of laws)
  - Advisable for businesses that can afford it to become involved to the extent that they can in the multi-stakeholder process

Thank You !