[TO BE PUBLISHED IN THE WM. MITCHELL LAW JOURNAL]

# Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration in Cyber-security Legal Frameworks: Reflections on the Proceedings of the Workshop on Cyber-Security Legal Issues at the 2010 United Nations Internet Governance Forum[1]

David Satola and Henry L. Judy[2]

The focus of this article is on exploring the evolution of best practices for developing international cyber-security legal frameworks. The article posits that due to the nature of the problems to be addressed, international legal responses to cyber-security should be developed in an on-going process whereby they are first deconstructed and approached in a modular fashion, and then integrated or re-integrated as consensus and political will develop. In a brief phrase, a dynamic "bottoms up" approach should be used. Among the problems with taking a comprehensive approach (or "top down" approach) to cyber-security legal frameworks is that the term means all things to all people, varies depending on the physical, educational and economic resources available in different jurisdictions, differs depending on the sensitivity of the data to be protected, needs to reflect different cultural expectations and priorities, among many other factors. In addition, it must be recalled that the whole area of cyber-security is both a relatively recent development as well as one that is notoriously in technological flux. While there is a continuing need for systematizing (and legal frameworks are simply a type of system), the very nature of subject resists systematizing or at least requires regular re-systematizing as the underlying reality alters with equal regularity.

Accordingly, while this article does not attempt to define "cyber-security" as a unitary concept, it does propose a hopefully deeper understanding of the issues comprising cyber-

[1] The content of this article is drawn in part from the proceedings of the Workshop on "Legal Aspects of Internet Governance: International Cooperation on Cyber-Security" held at the United Nations' 2010 Internet Governance Forum held at Vilnius, Lithuania, on September 15, 2010 ("Workshop") and the "Background Paper" prepared for the Workshop. Proceedings of the Workshop can be found at: http://www.intgovforum.org/cms/component/chronocontact/?chronoformname=WSProposalsReports2010View&wspid=123 . The "Background Paper" can be found at: http://www.afilias.info/webfm_send/135 .

[2] Henry L. Judy is Of Counsel at the international law firm K&L Gates LLP. David Satola is Senior Counsel in the Legal Vice Presidency a the World Bank. The authors are co-chairs of the Internet Governance Task Force of the Cyberspace Law Committee of the Section of Business Law of the American Bar Association. The views presented in this article are those of the authors in their individual capacities and do not necessarily reflect the views of the organizations with which they are associated or of any of the persons who participated as panellists in the Workshop or the organizations they represent. The authors would like to thank (i) Ali Zahid Ramin and Omar Martinez Sierra, both legal associates in the World Bank Legal Vice Presidency for early research on cyber-security themes; (ii) Jim Dempsey of the Center for Democracy and Technology, Lee Hibbard of the Council of Europe, and Veni Markovski for their contributions to the Background Paper; and (iii) the participants of the Workshop (in order of appearance) Vinton Cerf, Ivalo Kalfin, Rolf Weber, Alexander Seger, Jayantha Fernando, Ericke Itiarte, Andrew McLaughlin, Mike Silber, Bill Smith and John Morris.

security through a modular approach.  This article first looks at the landscape of current causes of, and threats to cyber-security.  In doing so, this article looks not only at what those threats are, but also looks at weaknesses “in the system” that may be exploited by, or that might exacerbate, those threats.  This article then looks at the main component parts (modules) of cyber-security (critical infrastructure protection, privacy, cyber-crimes, institutional matters, etc.).  It then looks at the current developments involving international responses and cooperative efforts with respect to each of the substantive areas (modules) and at recent attempts in the international sphere at addressing cyber-security legal frameworks incorporating those developments.  It concludes with some recommendations for a way forward.

## I. Cyber-security is a growing concern

In recent years, cyber-security has become a major and expanding concern of governments and the private sector around the world.  There has 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 cyber-attacks on key national infrastructure in Lithuania, Estonia, Georgia and other countries and on the databases of major global business corporations.[3]

- 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

[3] The seriousness of this concern is highlighted by the report “NATO 2020: Analysis and recommendations of the group of experts on a new strategic concept for NATO” at http://www.nato.int/strategic-concept/expertsreport.pdf.  The report recommends 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.

As the reach of the Internet continues to scale past a quarter of the world's population, and given the apparent sporadic user awareness on implementation of security protocols, systems operating on the Internet are often perceived as soft targets to a range of persons and 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 to the advancement for various causes.[4]

Cyber-crime 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 article. For example, recent developments involving the BlackBerry service of Research in Motion (RIM) and demands by the UAE, Saudi Arabia and India have uncertain effects on the ability of business and various professional to meet their legal obligations regarding trade secrets and confidential business information.[5] It has been recently reported that The United Arab Emirates' Telecommunications Regulatory Authority has the key for BlackBerry services and can decrypt and monitor BlackBerry communications after obtaining a court order and that RIM has reached a similar agreement with authorities in India.[6]

In terms of an evolving cyber-security legal framework, there are a number of evident vulnerabilities and impediments to effective international cooperation. Many of these were discussed in more depth at the Workshop.[7] Among these are:

- *Dissonance in national approaches to cyber-security*. Different countries, even members of the same regional organizations, can take different approaches to the concept of cyber-security in terms of the national policies, laws and implementation. Some countries see Internet governance as having state security at its core, by which they mean that the State can know exactly who sent and received every transmission, for every transmission what the traceroute was and what the contents of every transmission were; it can delete, block and/or seize any transmission of which it disapproves; and it can punish efficiently those who send or receive unapproved transmissions. At the other end of the spectrum other countries and organizations strongly believe that proper Internet governance, including Internet security, must be integrated and balanced with the type of freedoms protected by instruments such as the1st, 4th, 5th and 14th Amendments of the US Constitution, the EU Charter of Fundamental Rights

[4] The recent phenomenon of cause–based "leak sites," such as Wikileaks and Openleaks adds a new dimension to these issues. See New York Times archive at http://topics.nytimes.com/top/reference/timestopics/organizations/w/wikileaks/index.html.

[5] *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.

[6] Article source: http://www.sans.org/newsletters/newsbites/newsbites.php?vol=12&issue=98&rss=Y#sID200

[7] See, Workshop transcript, supra note 1.

and numerous UN human rights documents.[8] This “dissonance” can lead to a lack of effective coordination and can result in part because of a lack of multi-stakeholder participation in both policy-making and legislation.

- *Policy and implementation incoherence*. Even within 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 developed in an analog era simply do not apply in a digital era, 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 international cyber-security incidents.[9] 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*. Although it may be obvious, the fact that cyber-security issues may arise resulting from faulty (or “buggy”) software code, simple human error and sloppy behavior using the Internet merit mentioning in this panoply of causes of cyber-insecurity.[10] Legal systems have not developed a consensus on addressing responsibility for offering such code in the marketplace. It is often left to contract law and the software developer often writes the exculpatory software license. However, if the licensee has sufficient market power, the licensor may be exposed to significant contractual and tort liabilities for defective code.

- *Existing tools and instruments are not fully applied or are only partially implemented.* Another source of vulnerabilities in the existing cyber-security legal frameworks results from failure to apply the terms of existing instruments or only partial implementation of such instruments. Legal systems are increasingly responding to this source of vulnerability by establishing liability for failure to implement existing tools in a manner proportional to the sensitivity of the data held. This liability may be imposed because proportional security mechanisms were not employed as promised or regardless of whether a promise was made. However, this liability is often imposed on a case-by-case basis and not pursuant to statutory and regulation requirements aimed at the particular issue.[11]

[8] This topic is reviewed generally in U.S. Secretary of State Clinton’s January 1, 2010 “Remarks on Internet Freedom” at http://www.state.gov/secretary/rm/2010/01/135519.htm.

[9] 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.

[10] For a more thorough discussion of “buggy code” and the cyber-security problems caused by it and simple human error, see the comments of Andrew McLaughlin at the transcript of the Workshop (Transcript) at: http://www.intgovforum.org/cms/component/content/article/102-transcripts2010/661-123.

[11] See for example Federal Trade Commission (FTC) Decision and Order in the matter of Dave and Busters at http://www.ftc.gov/os/caselist/0823153/100608davebustersdo.pdf. See also FTC Agreement Containing Consent Order in the Matter of Twitter, Inc. at http://www.ftc.gov/opa/2010/06/twitter.shtm.

## II. A Modular Approach to the Main Themes of Cyber-Security

The cyber-security themes covered in this article are outlined below. This thematic analysis to cyber-security allows and lends itself to a modular approach to the issues covered. As will be demonstrated in this article, while there is good international practice in many of the themes covered, there is no one-size-fits-all approach; every country addresses "cyber-security" slightly differently. Deconstructing cyber-security along these thematic, modular lines – rather than attempting to identify one all-encompassing, comprehensive model – also allows for greater selectivity when crafting the legislative responses to policy choices. In addition, disaggregating the issues that comprise cyber-security lends itself to a better understanding of cyber-security issues, and therefore the ability to respond to them. 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 in the form of 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 cyber-security emerge from this analysis.

At the same time, it is important to recognize that a cyber-security legal framework needs to have an internal logical consistency; the bits and pieces need to work together. The modular and layered approach allows national policy-makers and legislators to tailor specific approaches to particular problems. It also allows policy-makers and legislators to prioritize on matters that are most important to managing cyber-security in their country.

In this section, we begin to explore the inter-relationships of these themes – for example, how security concerns play-off of privacy concerns and *vice versa*, how in crafting policy certain trade-offs are inevitable and how the manner in which these trade-offs are made by nation states results in itself in certain difficulties in enhancing international cooperation, in forging consensus and in the evolution of legal framework harmonization or inter-operability. Without casting judgment on these tradeoffs, it must at the same time be recognized by policy-makers, legislators and regulators at the national level, and by stakeholders at the regional and international level, that certain balances must be obtained for the legal regimes to function.

The themes are:

1. *Security – Critical Infrastructure Protection* - this section will focus on securing the infrastructure over which data and communications flow.

2. *Digital Data Protection* – this section focuses on certain key substantive issues around protection of digital data and database management. This analysis is not focused exclusively

See also FTC Settles with Twitter — More Painful Lessons in Basic Data Security at http://www.klgates.com/newsstand/Search.aspx?attorneys=b558c4c9-ad64-4ab0-bcbf-8eef081e96a9 and http://www.ftc.gov/opa/2010/06/twitter.shtm on “privacy” issues; it also includes protection of confidential and proprietary data generally. Legal frameworks that enable persons to control the manner in which data about them is handled are clearly important from many points of view, including protection of human rights and the availability of concrete mechanisms to do so, such as Opt-in/Opt-out clauses and so-called “Breach Notification” requirements. However, the ability of businesses and governments to function depends equally on the protection of confidential and proprietary data from inappropriate compromise.

3. *Cybercrimes & Enforcement* – the area of cyber-crimes is perhaps one of the more clearly identified thematic areas and the one where there is almost universal agreement on best practice, as inhered in the Budapest Convention.

4. Institutional Arrangements – finally, the article examines certain key institutional issues, mainly around critical infrastructure protection and data protection. This article does not address institutional issues regarding cyber-crimes, for example, because these are mainly dealt with in the context of the police and the jurisdiction of the criminal courts.

## III. Overview of Current Status of Cyber-Security Themes

Section III undertakes a brief substantive overview of the major cyber-security themes and surveys the institutions or organizations mainly responsibility for the evolution of international practice in those areas.

### A. Security- Critical Infrastructure Protection

This section III.A [12] deals with international legal aspects of critical infrastructure protection (“CIP”), in particular protection of critical information infrastructure (“CII”). [13] CIP

[12] See, generally, “The Potential for an International Legal Approach to Critical Information Infrastructure Protection”, Satola & Luddy, 47 Jurimetrics J. 315-333, ABA 2007 (Satola/Luddy). Certain parts of this section III.A.1. are based on and drawn from Satola/Luddy.

[13] For a working definition of these terms, *see*, Satola/Luddy at footnote 1, reproduced here: “Critical Infrastructure” and “Critical Infrastructure Protection” can be broadly defined. As used in thisarticle, Critical Infrastructure borrows from the definition found in the EU Green Paper, *On a European Programme for Critical Infrastructure Protection*, COM(2005) 576 of 17 November 2005 (the “Green Paper”), and as utilized in the Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks Against Information Systems (the “Council Decision”); *viz.*, infrastructure (including physical resources, services and information technology) is critical if the damage, destruction or disruption of the infrastructure asset would have a negative and serious impact on security. *See*, Green Paper, Annex 1. The Green Paper defines CII as “ICT systems that are critical infrastructures for themselves or that are essential for the operation of [other] critical infrastructures…” *Ibid.* Of particular relevance to the “cyber” context is the definition of an “information system” used in the Council Decision: an “’information system’ means any device or group of interconnected or related devises, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection or maintenance.” *See*, Council Decision, article 1(a). The CRITICAL INFORMATION INFRASTRUCTURE HANDBOOK (2006) (“CIIP Handbook”), at page 26, defines critical infrastructure and critical information infrastructure are those assets which if incapacitated or destroyed would have a debilitating impact on the national security and the economic and social welfare of a nation.”

is one area where cooperation is more evident at some levels than others. This may be because there are a greater variety of actors in the space (from the governmental, non-governmental, academic and private sectors) and it is an area that is thought of being more “technical” than “legal”. As noted in the literature:

> *“Best practice” regarding CIP is evolving, with interests of divergent stakeholders being served in different fora. For example, governments are interested in national security and the protection of public utilities, the private sector and business communities are interested in secure transactions, consumers and users are interested in protecting personal data, and technologists and engineers are interested in the stability of the network.”* [14]

Much of CII, including the Internet, is owned and operated by the private sector; while other critical infrastructure is owned by governmental or quasi-governmental entities. “Open” networks and technologies has increased the interdependence of an increasingly wider range of stakeholders using the Internet and threatened or at least made more vulnerable traditional constructs of the Westphalian “state” in attempting to isolate and deal with cyber-security issues.[15]

### 1. International Cooperation

The private, governmental and non-governmental sectors, on the basis of both national and international efforts, have been taking steps to increase the security of their products, services and networks. These efforts include, for example, the work of international standards bodies, which range from the treaty-based International Telecommunication Union (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. Internationally, a consensus appears to be emerging around both the process and substantive elements of CIP.[16] In terms of substantive elements, CIP is

[14] Satola/Luddy at 317.

[15] As pointed out in Satola/Luddy, “This sector-specific, ‘proprietary’ national approach in a world dominated by converged technologies is increasingly anachronistic.”; citing, Robert Bruce et al., World Bank Group, Cyber Security: A New Model for Protecting the Network 8 (2006) , at page 316, fn 2 and accompanying text.

[16] *See, generally,* Satola/Luddy at pp 318-319. *See, also,* (i) the “Culture of Security guidelines” of the OECD (OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture Of Security (2002) http://www.oecd.org/dataoecd/16/22/15582260.pdf (“OECD Guidelines”); the OECD Background Report on the Future of the Internet: Discussion Paper, Budapest, Hungary 4-5 October 2006 ); and the UN Resolutions on Cyber Security (ii) United Nations General Assembly Resolution 57/239, Creation of a Global Culture of Cybersecurity, 57th Session, 31 January 2003, available at: http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_57_239.pdf ; United Nations General Assembly Resolution 56/121, Combating the Criminal Misuse of Information Technologies, 56th Session, 23 January 2002, available at http://www.unodc.org/pdf/crime/a_res_56/121e.pdf ; and United Nations General Assembly Resolution 55/63, Combating the Criminal Misuse of Information Technologies, 55th Session, 22

aimed at ensuring that disruptions to CII be brief, infrequent, isolated and minimally detrimental.[17] This was highlighted by participants in the Workshop. Second, CIP should be dynamic and "process-oriented"[18]

Although the rate of adoption has not been as rapid as one might ideally want, successful efforts by the Internet Corporation for Assigned Names and Numbers ("ICANN") 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.[19]

Computer Emergency Response Teams ("CERTs") are generally cooperative endeavors among governments, academic institutions and commercial entities consisting mainly of technologists aimed at identifying cyber vulnerabilities and defending against cyber-attacks.[20] 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 (FIRST)[21] is an international non-governmental organization that seeks to promote global cooperation and coordination among these teams. Its membership includes over 200 teams across 28 countries. FIRST is an international organization bringing together a number of national CERTs.[22] It provides a forum for information sharing among CERTs and other incident response organizations, and is also a repository of technical and other information about CIP. As such, FIRST is an example of enhanced international cooperation in the area of cyber-security.

The European Government CERTs (EGC) Group has 11 member organizations.[23] 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.

CERTs typically focus on technical issues and their main function is information sharing providing primarily early warning functions.[24] In parallel, as the legal framework around CIP evolves, continued improvements in cooperation and consultation will be necessary in order to guard against differences in laws or the legal frameworks of countries resulting in divergences that would hinder rather than aid effective CIP. Different interest groups (stakeholders) need to talk to each other to ensure real, effective cyber-security and to avoid a divergence in approach

January 2001, available at http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf.

[17] *See*, Green Paper, at p. 1.

[18] See, generally, Smedinghoff, *supra* note 7 for a discussion of what is entailed in process-oriented approaches.

[19] *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.

[20] Satola/Luddy, at 319.

[21] http://www.first.org

[22] *See*, generally, http://www.first.org .

[23] http://www.egc-group.org

[24] Satola/Luddy.

to CIP. [25] As is already recognized by the literature, coordination, collaboration and consultation are key.

As was pointed out in the Workshop, many countries certain elements of the legal enabling environment addressing cyber-security, but these national legal frameworks vary widely in terms of the the manner in which cyber-security issues are addressed. Moreover, even where countries do have specific provisions dealing with CIIP, differences exist between countries as to how CII is to be protected. The modules identified in Section II., above (CIP, digital data protection, cybercrimes and institutional aspects), remain the focal points of evolving best practice.[26]

### 2. US Private, Governmental and Non-Governmental Cooperation

Perhaps the central lesson regarding CIP that emerged experimentally is that the effectiveness of any CIP program is directly proportional to the extent of cooperation among key private, governmental and non-governmental actors. However, no general standards for such co-operation have emerged. Perhaps the most comprehensive and detailed instance of this form of cooperation is provided by the U.S. Comprehensive National Cybersecurity Initiative (CNCI).[27]

The CNCI began in 2008 under the Bush Administration when the President issued National Security Presidential Directive 54 (*a.k.a.* Homeland Security Presidential Directive 23) on January 8, 2008. The directive called for the formation of the CNCI. The Bush administration developed CNCI to improve how the federal government protects sensitive information from hackers and nation states trying to break into agency networks and critical national infrastructure. Development of the CNCI continued under the Obama administration and on March 2, 2010 the White House published an unclassified summary of its CNCI, indicating that it consisted of the following 12 “initiatives.” These included Initiative #2 to deploy an intrusion detection system of sensors across the Federal enterprise and Initiative #3 to pursue deployment of intrusion prevention systems across the Federal enterprise.[28]

To implement Initiatives #2 and #3 the U.S. federal government developed and deployed the Einstein Program. In general, Einstein is an intrusion detection system that monitors the Internet network gateways of government departments and agencies in the United States for unauthorized traffic and malicious content. The original deployment was Einstein 1. The current deployment is Einstein 2, which conducts automatic full packet inspection of traffic entering or exiting U.S. Government networks using signature-based intrusion detection

[25] This phenomenon was noted with respect to cyber-crime legislation by the European Union in the Council Framework Directive on attacks against information systems, 2005/222/JHA of 24 February 2005.
[26] Satola/Luddy at 321.
[27] It should also be noted that 2010 saw a number of bills being introduced in the 111th U.S. Congress dealing with institutional issues, coordination of cyber-security and protection of CII at the level of the federal government level, as well as development of human capacity in the area of cyber-security. Among these are, for example, Senate Bill , "Protecting Cyberspace as a National Asset Act”, and House Bill, "Homeland Security Cyber and Physical Infrastructure Protection Act". It could therefore be expected that the 112th Congress may take some legislative action in these areas.
[28] See http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

technology. Einstein 2 is capable of alerting US-CERT in real time to the presence of malicious or potentially harmful activity.

Einstein 3 is currently being deployed on a limited pilot program basis and adds the additional capability to do real-time, full, deep packet inspection and to respond appropriately to cyber threats before harm is done, providing an intrusion prevention system supporting dynamic defense. In addition, when deemed necessary by the Department of Homeland Security (DHS) Einstein 3 can send alerts that do not contain the content of communications to the National Security Agency (NSA) so that DHS efforts may be supported by NSA. Einstein 2 is based predefined attack signatures that come from internal, commercial and public sources. Under Einstein 3 DHS will be able to adapt threat signatures determined by NSA in the course of its foreign intelligence and Department of Defense information assurance missions. Intrusion detection systems require signatures of malicious traffic, allowing the system to search traffic flows for those malicious configurations. One advantage of Einstein 3 is that it connects to intelligence sources to provide a fuller list of signatures.

Einstein 3 may also be deployed to monitor government computer traffic on private sector sites and Defense Department officials have suggested that Einstein 3 be used to provide CIP in the private sector, particularly with respect to CII such as CII serving the financial, utility and communication industries.[29]

The Einstein Program, and most particularly Einstein 3, has raised concerns among a number of privacy and civil liberties groups, particularly with the added capacity for deep-packet inspection, data sharing with NSA and extension of the program to the private sector.[30]

In addition, concerns have been raised regarding a program called “Perfect Citizen” that is being implemented by Raytheon under a $100 million classified contract with NSA to help assess the vulnerabilities and capabilities of networks of domestic US “critical infrastructure” such as utilities and nuclear power plants, both private and government run. This is a response to increasing concern by intelligence officials about foreign surveillance of computer systems that control the electric grid and other U.S. infrastructure. Google is partnering with NSA to help Google analyze the major corporate espionage attack that recently targeted its computer networks.[31]

The essential issue presented here is what the boundaries to “cooperation” are or the boundaries to the forms of cooperation. There is an obvious and difficult tension between the State’s responsibility for public safety and the citizen’s “right to be left alone” by the State. While these issues have been widely discussed and congressional hearings have been held, no consensus or resolution has emerged. The tension is an ancient one, but the resolution of the

[29] See http://www.wired.com/threatlevel/tag/einstein/#ixzz0v0uV4JWa

[30] See http://www.cdt.org/security/20090728_einstein_rpt.pdf. See Privacy Impact Assessment for Einstein 2 http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf. See Privacy Impact Assessment for the Initiative Three Exercise March 18, 2010 at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3.pdf.

[31] See February 4, 2010 Washington Post article “Google to enlist NSA to help it ward off cyberattacks” at http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html.

tension is far more difficult and consequential in the age of global cyber-security. How these issues are being handled in the United States is but one example, albeit an illustrative one, of how the contours of the debate are taking shape. As suggested throughout this article, these issues continue to evolve in a dynamic fashion.

### B. Digital Data Protection – Striking a Balance

A key area dealt with in cyber-security legislation is the protection of digital data. This area may be thought of in terms of confidentiality of digital data generally and in terms of personal data more specifically. The more general term would include protection of trade secrets and other forms of intellectual property, protection of confidential client information, and protection of the sensitive or proprietary information of businesses and governments. The latter refers to information by particular human beings may be identified according to the standards of different jurisdictions. The latter is referred to be various terms, such as privacy, protection of private life, protection of personal information and data protection and presents complex technical issues, such as the issue of "attribution," - the extent of the ability to determine the true senders of any message or request for information.[32] It appears that greater cross-border cooperation in the area of digital data protection could be achieved. Though hard evidence is not available, the reasons hampering greater cooperation seem to revolve around the question of the balance, the trade-offs, between data protection and security and go to the core of the relationship between the individual and the state. This may make international cooperation more difficult.

#### 1. Data Confidentiality

The protection of confidential digital data is critical to the functioning global commerce and government on every level. It has been estimated that more than half of the value of US businesses lies in their trade secrets and other intellectual property and that the value of the trade secrets and intellectual property comprised each year are in the billions of dollars. Private firms and other companies with fiduciary and near fiduciary obligations (law and accounting firms, for example) must be able to communicate confidentially. Even governments may have a need for confidential communications, and the Wikileaks cases of 2010 have, ironically, laid bare both the sensitivities and the corresponding necessities regarding protecting data confidentiality in the Internet age.

It is basic principle of knowledge management that appropriate sharing of information enables organizations to make smarter decisions and produce more successful results, and that inappropriate sharing and inappropriate restrictions on sharing produces an increased risk to them of adverse consequences, including less intelligent decisions. While the various Wikileaks cases may have been aimed at uprooting the "conspiratorial nature" of governments[33], they clearly demonstrate that organizations are information-gathering and information-processing machines and information is a tool that can be used as a weapon or beneficently. It remains to be

[32] This article focuses only on data in digital or electronic form. Nevertheless it is recognized that confidential and personal data is regularly held in hard copy form and that many of the considerations and legislative acts discussed apply equally to hard copy.

[33] See Assange, Julian "State and Terrorist Conspiracies" (November 10, 2006) at http://iq.org/conspiracies.pdf

seen what the effects of this type of use information will have on organizations in terms of their information gathering, dissemination and especially information security processes and procedures. These incidents also highlight the hard balancing issues of what sharing, restriction and therefore security practices are appropriate for different types of organizations, different types of and information and in different contexts and time. Thus we see real case examples of the benefits of looking at these cyber-security questions in a more disaggregated and modular way.

## 2. Protection of Personally Identifiable Information ("PII")

The scope of the concerns that are inherently involved in the topic of PII protection is enormous - freedom of speech, freedom of expression, access to information, political speech, censorship, personal data collected for police or other surveillance purposes, Internet filtering, censorship, political speech on-line the treatment by third parties (data processors) of the collection, processing and dissemination of data in digital format of an individual (data subject). Data subjects are real people and not juridical persons or other "constitutional" aspects of privacy. The focus of the report is not a "rights-based" or constitutional analysis.

The trend globally in legal frameworks regarding PII protection has been towards the adoption of a "constitutional" approach, balancing the "privacy" interests of the individual vs. security and other policy interests that the state has, or wishes to foster or avoid restricting. This constitutional approach is inherent in the European Directives and the Council of Europe (CoE) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Privacy Convention). [34] Even India – which currently has only very limited legislation specifically dealing with PII protection – uses a constitutional approach to protecting privacy.[35]

That said, however, much of available good international practice in terms of the treatment in legal frameworks of digital data are based in the constitutional approach to privacy, as is the case, for example, in the EU and by the Council of Europe (both discussed in more detail, below). Notwithstanding the rights- and constitutional bases of legal treatment of digital data, this report looks to the mechanics of how different national laws deal with different aspects of the treatment of digital data. Treatment of digital data is in any case an essential part of creating a cyber-security legal and regulatory enabling environment.

There is a great deal in the media currently regarding privacy in the digital age. Indeed one outgrowth of the UN's Internet Governance Forum (IGF) was the creation of a so-called Privacy Dynamic Coalition. Just prior to the IGF meeting in Sharm el Sheik in November 2009, the Coalition along with civil society groups and other privacy experts promulgated the so-called "Madrid Privacy Declaration"[36] affirming privacy as a fundamental human right. While the Declaration takes a fairly wide sweep on privacy issues in the digital age, it also urges countries that have not yet established a comprehensive framework for privacy protection and an

[34] http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm

[35] For a comprehensive discussion the current state of Indian privacy protection, see the Indian Government's draft discussion paper entitled "Approach Paper for a Legislation on Privacy" dated October 13, 2010 at http://persmin.gov.in/WriteReadData/RTI/aproach_paper.pdf

[36] http://thepublicvoice.org/madrid-declaration/

independent data protection authority to do so as expeditiously as possible. It also urges countries that have not done so to adopt the CoE Privacy Convention. The Privacy Convention was opened for signature in 1981.

Among the key digital data issues dealt with from a cyber-security point of view in this report are (i) protections against secondary use and (ii) notification in case of breach of digital “privacy”. A third area of digital data protection explored in the report, as will be seen from the country benchmarking section, is the variety of institutional forms that have been put in place in response to these digital data concerns.

Many countries have established data or privacy commissioners. International practice in this area, as with many others explored in this report, shows that there is no one-size-fits-all approach.

In this regard, for example, there is a major schism between the United States on the one hand and Europe (and other countries) on the other, in terms of the structure of privacy and the regulation of how data is gathered and used. To generalize considerably, in the United States, privacy law is applied differentially depending on the economic or business sector and on the type of personal data. For example, different laws are applied to personal data held by financial institutions, educational institutions, health care providers, drivers license data, video rental data, etc. In Europe personal data is regulated in general terms regardless of these distinctions pursuant EU-wide Directives.[37] U.S. law in general tends to be more permissive about the level and timing of the consent of the data subject that needs to be given about the personal data that may be collected and shared. The law in Europe and in countries following the European model tends to be less permissive in that regard. To bridge this gap, the U.S. Department of Commerce and the European Commission have developed a "safe harbor" framework of data protection principles ("Safe Harbor")[38]. This safe harbor is designed to provide U.S. organizations with a means to satisfy the European Union's legal requirement that “adequate” data protections be afforded to personally-identifiable information transferred from the European Union to the United States, since US is not considered to be adequate in that regard.

Regardless of the differences in systems and approaches, certain principles can be distilled from the variegated practices. In terms of managing one’s own data, a data subject should be enabled through the legal framework to be able to verify the data about him/herself and make such corrections as are necessary in a timely and transparent fashion. In the words of one scholar, a data subject should not be “excluded” from his/her own data.[39]

[37] See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML.

[38] See Safe Harbor materials at http://www.export.gov/safeharbor.

[39] Solove, Daniel, “Understanding Privacy”, Harvard 2008, at 134-5.

Data breach notification is another area of concern to data subjects, policy-makers and regulators around the world, and, again, practice is varied. Even in the EU (under the umbrella of a common framework Directive) there are a variety of approaches to data breach notification. First there must be a determination of the nature of the data that is subject to protection. This depends on how "personal data" is defined in the law. Then a determination needs to be made as to what information about the person is covered and what exceptions, if any exist. For example, "public" information would probably not be covered, but that depends on what the definition of "public" is. Next is a determination of what constitutes a "trigger" for a breach notification – how is it determined when data about a person has been acquired by a third party in an unauthorized fashion under the law, as well as any exceptions? If a notice obligation applies, to whom does the notice of breach go? To the data subject or to the data intermediary? At what time must the notice be given, in what form and how much detail about the breach must be included in the notice. Finally, what are the remedies to be provided and how and by whom are they enforced?

A number of info-Security standards are being developed that may apply here as well. These include the practices of bank/credit card industry, and even the International Standards Organization (ISO) (for example, ISO 17799). [40]

### 3. Developments in the EU and the US

In the EU, the protection of PII is the subject of the EU's Framework Data Protection Directive 95/46/EC (Directive). The Directive regulates secondary use of data requiring that data must be "collected for specified, explicit and legitimate purposes and not further processes in a way incompatible with those purposes."[41] One of the main purposes of the Directive was to achieve harmonization across the EU. In the EU, the article 29 Working Party on Data Protection provides advice concerning the meaning and application of the Directive, including whether Member States are compliant with the Directive.

The European Commission conducted a public consultation in 2009 on "the legal framework for the fundamental right to protection of personal data." As stated in the report[42] on the consultation, "The Directive was developed at a time before the full commercialization of the Internet and when many of the technologies underlying much modern data processing were still experimental." The review went further and concluded that these changes did not result in any need to address the underlying fundamental principles of data protection (including the principles found in the OECD Guidelines (discussed in 3., below)), but recognized that the certain elements of the Directive could be updated to simplify processes and "[adjust] the legal framework to take account of changes in the handling of personal information brought about by 15 years of technological change."[43]

As a result of this consultation on November 4, 2010 the EU Commission issued a Communication to the EU Parliament and the Council, "A comprehensive approach on personal

[40] *See* http://www.iso.org/iso/home.html.
[41] Directive, art. 6.
[42] http://ec.europa.eu/justive_home/news/consulting_public/news_conuslting_0003_en.htm
[43] *Id.*

data protection in the European Union."[44] The Communication proposes a wide-ranging and fundamental update of EU data protection law. Less than a month later on December 1, 2010, the US Federal Trade Commission ("FTC") released a preliminary staff report entitled "Protecting Consumer Privacy in an Era of Rapid Change" ("FTC Proposal").[45] The FTC Proposal sets forth a broad new framework which, like the EU Communication, suggests wide-ranging and fundamental revisions to US privacy law.

Although there are a number of differences between the FTC Proposal and the EU Commission's Communication, their most notable feature is their commonalities, including an emphasis on prior consent, stronger remedies for violations of privacy and the role of changes in technology in driving the need for changes in privacy law. Both focused strongly on the role of "profiling", that is, the use of technologies for data gathering and analysis and related business and governmental practices that enable the creation of "profiles" that have the same effects for all practical purposes as gathering obviously personal information. The Communication also focused on the effects of cloud computing on privacy law.

A principal factor in driving this tendency toward increasing convergence in the US and EU legal regimes for data protection is the high level of integration of the US and EU economies, as reflected in the number of corporate offices in each other's jurisdictions and the significant personal data flows between the two economies. This integration is one of the reasons for a forthcoming Internet privacy report from the US Department of Commerce that is expected to inform policy decisions by a recently created White House Privacy and Internet Policy Subcommittee. This Subcommittee is expected to address and seek to coordinate the direction of US federal law on privacy regulation for the standpoint of the Executive Branch.[46]

### 4. CoE Convention

The Privacy Convention is the only international treaty dealing specifically with data protection. It is mainly a European instrument, although it is open to signature by countries outside of Europe. One key feature of the convention is that it is not self-executing; *i.e.*, adherents to the Privacy Convention would need to incorporate its principles into national legislation. For example, similarly to the EU Directive, the Privacy Convention requires that data be "stored for specified and legitimate purposes and not used in a way incompatible with those purposes."[47] On the specific subject of profiling, November 24, 2010, the Committee of Ministers of the Council of Europe adopted a recommendation to all members states that profiling be permitted, subject to certain exceptions, only if "the data subject or her or his legal representative has given her or his free, specific and informed consent."[48]

[44] The Communication is available at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.

[45] The report is available at http://ftc.gov/os/2010/12/101201privacyreport.pdf.

[46] See recent Congressional testimony by Daniel Weitzner, Associate Administrator for policy at the National Telecommunications and Information Administration, at http://energycommerce.house.gov/documents/20101202/Weitzner.Testimony.12.02.2010.pdf.

[47] Privacy Convention, art. 5b.

[48] See recommendation at https://wcd.coe.int/wcd/ViewDoc.jsp?Ref=CM/Rec(2010)13&Language=lanEnglish&Ver=original&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383.

### 5. Asia-Pacific Economic Cooperation

Asia-Pacific Economic Cooperation ("APEC") is a forum that was established in 1989 for twenty-one (21) Pacific Rim countries that seeks to promote free trade and economic cooperation throughout the Asia-Pacific region.[49] They are referred to as "Member Economies". The population of 21 Member Economies is in excess of 2.7 billion people and the Member Economies represent approximately 54 percent of world real GDP and 44 percent of world trade.[50] APEC's activities are focused on three key areas: trade and investment liberalization, business facilitation and economic and technical cooperation. In support of these goals, APEC has established the APEC Privacy Framework ("Framework")[51]. Although the Framework speaks to privacy regulation within Member Economies, its focus is on information sharing between and among economies; on cooperative development of a system of cross-border privacy rules for use by businesses and on developing arrangements for cross-border cooperation in investigation and enforcement. The Framework addresses privacy as a consumer protection and trust issue rather than from the standpoint of human rights and civil liberties and places heavy reliance on self-regulation.

Recently APEC established a Cross-border Privacy Enforcement Arrangement ("CPEA")[52] that facilitates information sharing and cooperation between authorities responsible for data and consumer protection in the APEC region. The CPEA was endorsed by APEC Ministers in November 2009 and commenced operation on 16 July 2010. The initial signatories, that is, participating privacy enforcement authorities were the Australian, New Zealand, Canadian and Hong Kong Privacy Commissioners and the US Federal Trade Commission.[53]

Many privacy advocates do not regard the Framework, the CPEA and APEC's other privacy oriented projects as providing an appropriate level of protection, especially with respect to the most recent technological challenges. However, it is also generally recognized that APEC's initiatives represent significant forward steps in privacy protection, particularly in a number of the less developed countries in the region and may constitute valuable building blocks for further evolution of this legal framework.

### 6. Other International Sources

Another source of data protection principles is the OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data (Guidelines).[54] The

[49] http://www.apec.org

[50] See "APEC at a Glance, 2010/2011" available for free download from the APEC website at http://publications.apec.org/publication-detail.php?pub_id=1077

[51] See copy of Framework at http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf

[52] The full text of the CPEA is at http://aimp.apec.org/Documents/2010/ECSG/DPS1/10_ecsg_dps1_013.pdf; for further information regarding the CPEA, see Fact Sheet at http://www.apec.org/About-Us/About-APEC/Fact-Sheets/Collection/APEC-Cross-border-Privacy-Enforcement-Arrangement.aspx.

[53] See "FTC Joins New Asia-Pacific Multinational Network of Privacy Enforcement Authorities" at http://www.ftc.gov/opa/2010/07/apec.shtm

[54] *See*, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html .

Guidelines are built around eight principles for treatment of personal data: collection (limits the means by which data are collected), data quality (this has to do with the relevance of the data collected), “purpose specification” (this requires that the purposes for which data are collected are known in advance and subsequent use is limited to those purposes), use limitation (this limits disclosure of data), safeguards (this protects data against risk  of loss or unauthorized access), openness (this relates to the operational standards of the data controller), individual participation (this sets forth the rights of the “data subject” over his/her own data) and accountability (imposed on data controllers).   The Guidelines form the basis of the legislative framework in Canada, for example.

Finally it is important to note that, at the two most recent meetings of the International Conference of Data Protection and Privacy Commissioners, the Conference has adopted resolutions with respect to the adoption of binding global privacy standards and facilitating cross-border enforcement actions.  Perhaps the most comprehensive and substantive of these resolutions is the so-called “Madrid Resolution” adopted in November 2009.[55]

### C. Cybercrime – The Law Enforcement Response

International best practice, if not international cooperation and collaboration, are more evident in the area of cybercrime, perhaps in part to the near universality of the substantive provisions of the Budapest Convention (defined below).

#### 1. International Experience

At the recent 12th pentennial UN Crime Congress[56] held in April 2010 in Salvador, Brazil, efforts to negotiate a global cyber-crime treaty were unsuccessful despite intense discussion among the parties. A number of major powers disagreed over national sovereignty issues and concerns for human rights.  For example, the Budapest Convention permits police under certain circumstances to cross national boundaries to access servers without consent from local authorities.  Russia, for example, asserted that permitting foreign law enforcement agencies to conduct Internet searches inside Russian borders violated the Russian Constitution.  In addition, because of phenomena such as cloud computing, which can result in data being transferred across national boundaries to servers in any location, police from one country can be denied access to data in a foreign location. Other countries insisted on the need for privacy provisions that would protect users' data from police investigation when it is stored in another country via a cloud computing partner.

These and other issues present countries with inherently conflicting policy objectives and cultural clashes including the need to balance different interests and rights such as security and privacy, compounded by the impact of rapidly developing technologies on the structure of any agreement.  The resolution of issues on this level suggests the need for the kind of bottom-up approach suggested by this article.

[55] *See* Madrid Resolution at http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf.

[56] *See*, http://www.unodc.org/unodc/en/crime-congress/12th-crime-congress.html

### a. Council of Europe

In the area of cyber crimes, the 2001 Convention of the Council of Europe ("CoE Convention or the "Budapest Convention")[57] is a historic milestone *vis-à-vis* cyber security and cybercrime and provides a nearly universal standard of good international practice regarding legal frameworks for the protection against "cyber-crimes". Although the Convention was promulgated under the auspices of the Council of Europe, it is open to signature by any country. In fact, a number of non-CoE countries (for example, the Unites States) have not only signed, but ratified the Convention.

The Convention addresses three sets of issues: the categories of cyber-crime 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. Moreover, according to the COE, some 100 countries have made use of the Budapest Convention when developing national cyber-crime legislation.

Cyber-crime 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 cyber-crime context.[58] 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."

The Convention consists of four chapters:

- **Chapter I** titled *"Use of terms"* includes definitions of *"computer system"*, *"computer data"*, *"service provider"* and *"traffic data."*

- **Chapter II** titled *"Measures to be taken at the national level"* consists of three sections -- "*Substantive criminal law*" (Section 1), "*Procedural law*" (Section 2) and "*Jurisdiction*" (Section 3). All sections in the Convention are further subdivided into *"Titles."* The section on *substantive criminal law* is divided into 5 titles with the first four titles classifying different types of offences:

  - *"Offences against the confidentiality, integrity and availability of computer data and systems*", which include offences such as *illegal access*, *illegal interception*, *data interference*, *system interference* and *misuse of devices*.

  - *"Computer related offences"*, which include *forgery* and *fraud.*

[57] *See*, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=1&DF=01/09/2009&CL=ENG

[58] *See,* http://www.guardian.co.uk/world/2010/jul/21/gary-mckinnon-extradition-david-cameron.

  - *"Content-related offences"*, which include offences related to *child pornography*.

  - *"Offences related to infringements of copyright and related rights*."

- The section on *procedural law* includes *"Common provisions"* (Title 1) that apply to the Convention's articles on substantive criminal law, and to other criminal offences committed by means of a computer system, and to the collection of evidence in electronic form relating to criminal offences. There is also a title on *"Expedited preservation of stored computer data"* and the section also includes provisions dealing with *"Production order"*, *"Search and seizure of stored computer data"*, *"Real-time collection of traffic data"* and *"Interception of content data."*

- **Chapter III** on *"International co-operation"* includes general principles relating to *"international cooperation"*, *"extradition"*, *"mutual assistance"* and *"spontaneous information"*. The chapter also contains procedures pertaining to *"…requests for mutual assistance in the absence of applicable international agreements"*, and to *"Confidentiality and limitation on use"* including Specific Provisions (Section 2) on *"Mutual assistance regarding provisional measures"* (Title 1), *"Mutual assistance regarding investigative powers"* (Title 2) and on a *"24/7 Network."*

- **Chapter IV –** *"Final provisions"* contains standard provisions found commonly in Council of Europe treaties. Importantly, in accordance with Article 40, any state may declare that it avails itself of the possibility of requiring additional elements, as provided for under certain articles.

In accordance with Article 42, any state may declare that it avails itself of the reservations provided for in certain articles. By ratifying or acceding to the Convention, countries agree to ensure that their domestic laws criminalize the conducts described in the section on substantive criminal law, and establish the procedural tools necessary to investigate and prosecute such crimes.

The Convention uses technology neutral language, so that it applies and covers both current and future technologies. States may exclude petty or insignificant misconduct from the offences it defines. Offences must be committed intentionally for criminal liability to arise. Additional specific intentional elements only apply to certain offences - for instance, to computer-related fraud, with the requirement of fraudulent or dishonest intent of procuring economic benefit.

International coordination and cooperation are necessary for the prosecution of cybercrime and other information security and network security issues and governments must take innovative steps to curb this serious threat. Offences must be committed "without right", referring to conduct undertaken without authority or conduct not covered by established legal defenses, excuses, justifications or relevant principles under domestic law. These definitions are not intended to criminalize legitimate and common activities inherent in the design of systems and networks, or legitimate operating or commercial practices.

### b. ITU

There are many resources interpreting and summarizing the Convention. In addition at the international level, the ITU has taken a leading role in collecting and synthesizing experience regarding cyber-crime legislation in its Guide and Toolkit.[59]

The ITU in conjunction with other partners took the leading role in organizing the World Summit on the Information Society (WSIS)[60] which was held in two phases: in Geneva in 2003 and Tunis in 2005. Governments, policy-makers and experts from around the world shared ideas and experiences about how best to address the emerging issues associated with of the development of a global information society, including the development of compatible standards and laws.

The outputs of the Summit are contained in the *Geneva Declaration of Principles*, the Geneva Plan of Action, the *Tunis Commitment* and the *Tunis Agenda for the Information Society*. Under the Tunis Agenda for the Information Society, the ITU was entrusted to take the lead as the sole facilitator for WSIS Action Line C5: "*Building confidence and security in the use of information and communication technologies (ICTs).*"[61] The ITU Secretary General launched the Global Cybersecurity Agenda (GCA) in May 2007 as a global framework for dialogue and international cooperation aimed at proposing strategies to enhance security in the Information Society.

### c. The Commonwealth

In an effort to harmonize computer-related criminal law in the Commonwealth countries[62] experts gathered to present a model law at the *Commonwealth Conference of Ministers* in 2002. Importantly, the model law, titled the *Computer and Computer Related Crimes Bill*, [63]shares the same framework as the Convention to limit conflicting guidance. It serves as an example of common principles each country can use to adapt framework legislation compatible with other Commonwealth countries.

A further Meeting of Senior Officials of Commonwealth Law Ministers was held in October 2007 to address laws to combat terrorism and money-laundering, which included discussion on cybersecurity / cybercrime.

[59] *Cybersecurity Guide for Developing Countries* – Edition 2007 – International Telecommunication Union. http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-e.pdf; see also, http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.

[60] http://www.itu.int/wsis/index.html

[61] Outcome documents are available at *id.*

[62] *See*, www.commonwealth.org

[63] The model law is accessible at http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD25204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf

### d. The United Nations Convention against Transnational Organized Crime (CTOC)

The CTOC was adopted by General Assembly Resolution 55 / 25 of 15 November 2000. It came into force on 29 September 2003.[64] It is the main international instrument in the fight against transnational organized crime, and seeks to promote international cooperation to prevent and combat transnational organized crime more effectively. Here, it merits noting that the CoE Convention is aimed at strengthening domestic, internal law regarding cybercrimes, while the CTOC Conventions is aimed at cross border criminal activity.

Although the COTC Convention does not provide a single, agreed definition of organized crime *per se*, its provisions do provide elements of a concept of organized crime. For instance:

- An organized criminal group is defined as three or more persons working together to commit one or more serious crimes in order to obtain financial or other material benefit.

- Transnational crimes are defined as:

  - offences committed in more than one State;
  - offences committed in one State, but a substantial part of preparation, planning, direction or control takes place in another;
  - offences committed in one State, but involving an organized criminal group that engages in criminal activities in more than one State; and
  - offences committed in one State, but having substantial effects in another State.

- Serious crime is defined as conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty.

### e. United Nations system decisions, resolutions and recommendations

Some additional relevant United Nations system decisions, resolutions and recommendations include[65]:

- The United Nations Commission on Crime Prevention and Criminal Justice (CCPCJ)[66] 2007 - Resolution 16/2 of April 2007 on *"Effective crime prevention and criminal justice responses to combat sexual exploitation of children"* (notably, paragraphs 7 & 16).

- The United Nations Economic and Social Council (ECOSOC)[67] Resolution E/2007/20 of 26 July 2007 on *"International cooperation in the prevention, investigation, prosecution*

[64] http://www.unodc.org/unodc/en/treaties/CTOC/index.html

[65] This list is non-exhaustive.

[66] See, http://www.unodc.org/unodc/en/commissions/CCPCJ/index.html

[67] See, http://www.un.org/ecosoc/

*and punishment of economic fraud and identity-related crime (E/2007/30 and E/2007/ SR. 45)".*

- ECOSOC Resolution 2004/26 of 21 July 2004 on *"International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes".*

- The *"Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first century"* (paragraph 18), endorsed by General Assembly Resolution 55/59 of 4 December 2000 and paragraph 36 of *"Plan of action for the implementation of the Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first century"* annexed to, and noted by, General Assembly Resolution 56/261 of 31 January 2002.

- The Bangkok Declaration on *"Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice"* (paragraphs 15 and 16), endorsed by General Assembly Resolution 60/177 of 16 December 2005.

- Recommendations of an ad hoc Congress Workshop on *"Measures to Combat Computer-Related Crime"*. Paragraph 2 of General Assembly Resolution 60/177 invited Governments to implement all the recommendations adopted by the Eleventh Congress.

- General Assembly Resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on *"Combating the criminal misuse of information technologies"*. This latter resolution invites Member States, when developing national law, policy and practice, to combat the criminal misuse of information technologies and to take into account, *inter alia*, the work and achievements of the CCPCJ.

- Various resolutions by the Commission on Narcotic Drugs,[68] including Resolution 48 / 5 on *"Strengthening international cooperation in order to prevent the use of the Internet to commit drug-related crime"* and Commission on Narcotic Drugs Resolution 43 / 8 of 15 March 2000 on the Internet. ECOSOC Resolution 2004 / 42 also addresses the *"Sale of internationally controlled illicit drugs to individuals via the Internet".*

- Paragraph 17 of the General Assembly Resolution 60/178 of 16 December 2005 on *"International cooperation against the world drug problem".*

- ECOSOC Resolution 2004 / 42 on the *"Sale of internationally controlled illicit drugs to individuals via the Internet".*

Subsidiary bodies of the Commission on Narcotic Drugs (e.g., the Sub-commission on Illicit Drug Traffic and Related Matters in the Near and Middle East and regional Heads of National Drug Law Enforcement Agencies (HONLEA) meetings) have also published relevant conclusions and recommendations. Additionally, the International Narcotics Control Board

[68] See http://www.unodc.org/unodc/en/commissions/CND/index.html

(INCB) published recommendations in its annual report for 2005 to curb the spread of illicit sales of controlled substances over the Internet, particularly pharmaceutical preparations.

### 2. Other Regional Experience

Regional experience can also inform the debate. In that regard, the following regional sources are highlighted here.

#### a. The League of Arab States

Several countries in Southwest Asia and North and Northeast Africa comprising the League of Arab States (Arab League for short) [69] have adopted cybercrime legislation, such as Tunisia[70], Saudi Arabia[71] and United Arab Emirates (UAE)[72].

From a regional perspective, the recently concluded *International Telecommunication Union ("ITU") Regional Cybersecurity Forum for Africa and Arab States*[73] held in Tunis, Tunisia in June 2009 (attended by ITIDA) serve to highlight some of the main challenges faced by countries in the region in enhancing cyber-security and securing critical information infrastructures. Importantly, it focused on the way forward for countries to strengthen their cyber-security frameworks[74].

#### b. The African Union

It is important to note that the African Union ("AU") [75] March 2008 *Study on Harmonisation of Telecommunication, Information and Communication Technologies Policies and Regulation in Africa*[76] identified the need for member countries to combat cybercrimes.

Many African countries have taken the initiative and forged ahead with legislation to address cybercrime and data protection.

## D. Institutional

The institutional arrangements supporting cyber-security are as varied and diverse as the approaches to the issues. Two points merit noting at the outset. First, there is no one-size-fits-all response to effective institutional design. As will be demonstrated, institutional arrangements

[69] See www.arableagueonline.org (English website under construction).
[70] Law No. 2004-5 of February 3 2004 relative to IT Security.
[71] See http://www.moj.gov.sa/adl/ENG/attach/28.pdf
[72] See http://www.aecert.ae/Prevention_of_Information_Technology_Crimes_English.pdf
[73] See http://www.itu.int/ITU-D/cyb/events/2009/tunis/index.html
[74] See http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/tunis-cybersecurity-forum-report-june-09.pdf
[75] See http://www.africa-union.org/
[76] See http://www.africa-union.org/root/ua/conferences/2008/mai/ie/11-14mai/draft%20report%20study%20on%20telecom%20ict%20policy%2031%20march%2008.pdf

vary dramatically. Second, as was mentioned in Section II, above, not all cyber-security issues have a specific institutional dimension. The most obvious one is the area of cybercrime, where practice indicates that issues of cybercrime, once passed into legislation, are usually within the purview of the police and the courts.

Briefly, the substantive areas that do lend themselves to special institutional arrangements including especially, CIIP (usually through CERTs) and data privacy protection (here practice is highly divergent).

CERTs, described in section III.A.1, above, are one of the main responses to protecting infrastructure. In some countries (ArCERT in Argentina, the Canadian Cyber Incident Response Center, MyCERT in Malaysia, SingCERT in Singapore, the Electronic Communications Security – Computer Security Incident Response Team in South Africa and TUNCERT in Tunisia), they take on a formal institutional role. These national CERTs also have various institutional reporting roles: ArCERT reports to the President through the National Office for IT. In Canada, CCIRC reports to the Prime Minister. MyCERT reports to the Prime minister through the Ministry of Science. Sing CERT reports to the Ministry of Information through the IDA. ECS-CERT I in South Africa reports to the President through the Minister of Data Secretary. TUNCERT reports to the Ministry of communications technologies through the National Agency for Computer Security.

In terms of privacy, a number of examples demonstrate the wide practice of institutional responses:

- ***Argentina***. In Argentina, the National Data Protection Directorate (NDPD) established under the Personal Data Protection Act is responsible for digital data protection[77]. The NDPD is under the Ministry of Justice and Human Rights.
- ***Canada***. In Canada at the federal level, the Personal Information Protection and Electronic Documents Act (PIPEDA) establishes the Office of the Privacy Commissioner of Canada (OPC) which reports to Parliament.
- ***European Union***. In the EU, generally, under the each country has a Data Protection Agency (DPA) principally responsible for the interpretation and enforcement of data privacy violations. Each DPA is typically an independent agency, with the authority to enforce against other government entities. For those EU member states with a criminal component to data protection legislation, national or regional prosecutors may be referred by the DPA for particular matters. In addition, at the EU level, there is a Working Party on Data Protection that determines which countries are compliant with the Directives.
- ***Malaysia***. In Malaysia, processing of personal data is regulated by the Personal Data Protection Act 2009 (PDPA). The Personal Data Protection Commissioner is appointed by the Ministry of Information, Culture and Communications and is in charge of implementing and enforcing the personal data protection laws in Malaysia.
- ***Singapore***. Singapore is an interesting case. There is no an overarching data protection or privacy law in Singapore. However, there are several industry-specific laws that deal with data protection and privacy issues and may be enforced by industry regulatory

[77] Law 25 326/00.

bodies. In addition, the Constitution of Singapore does not contain any explicit right to privacy although the High Court has ruled that personal information may be protected under a duty of confidence. Notwithstanding, the government of Singapore has been considering passing a comprehensive data protection act for more than ten years now[78].

- ***South Africa***. In South Africa, the Protection of Personal Information Act (PPIA) requires that personal information may only be processed by a responsible party that has notified the information Protection Regulator (Regulator) which reports to the President of South Africa.
- ***Tunisia***. In Tunisia, the Act on Protection of Personal Data establishes the National Authority for Protection of Personal Data (NAPPD). The NAPPD reports to the Ministry of Human Rights.

## IV. International, National and Organizational Responses

Having undertaken a brief substantive review of the themes and responsible institutions/organizations, this section IV provides a brief glimpse into some current responses to these issues.

### A. 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; and in many cases, this clarion call relates to issues of "cyber-war" and arise in a number of *fora*.[79] As noted above, NATO issued an experts report, "NATO 2020: Analysis and recommendations of the group of experts on a new strategic concept for NATO", 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.[80] The report contains the following blunt statements:

> *"NATO must accelerate efforts to respond to the danger of cyber attacks by protecting its own communications and command systems, helping Allies to improve their ability to prevent and*

[78] According to Privacy International's 2007 report on Singapore Available at: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559494

[79] In January 2010, Hamadoun Toure, former ITU Secretary General, 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?

[80] http://www.nato.int/strategic-concept/expertsreport.pdf

> *recover from attacks, and developing an array of cyber defence capabilities aimed at effective detection and deterrence."*[81]

> *"The most probable threats to Allies in the coming decade are unconventional. Three in particular stand out: 1) an attack by ballistic missile (whether or not nuclear-armed); 2) strikes by international terrorist groups; and 3) cyber assaults of varying degrees of severity."*[82]

> *"The Alliance should consider giving the Secretary General or NATO military leaders certain pre-delegated authorities, based on agreed rules-of engagement, to respond in an emergency situation such as a missile or cyber attack."*[83]

> *"The next significant attack on the Alliance may well come down a fibre optic cable. Already, cyber attacks against NATO systems occur frequently, but most often below the threshold of political concern. However, the risk of a large-scale attack on NATO's command and control systems or energy grids could readily warrant consultations under Article 4 and could possibly lead to collective defence measures under Article 5."*[84]

> *"....there persist serious gaps in NATO's cyber defence capabilities. The Strategic Concept should place a high priority on addressing these vulnerabilities, which are both unacceptable and increasingly dangerous."*[85]

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.[86]

When analyzing the merits of a treaty-based approach to cyber-security a myriad of questions arise, including: 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

[81] *Id.* at 11.
[82] *Id.* at 17.
[83] *Id.* at 35.
[84] *Id.* at 45.
[85] *Id.*
[86] *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-8dfe-670c0822a153/q_act_downloadpaper/q_obj_4112703c-47be-4d4d-93c2-8276ab2f35a3/display.aspx?rs=enginespage.

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.[87]

Various proposals are emerging for improving regional and international cooperation, including the following examples:

- 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.[88] 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 cyber-crime.[89]

- 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".[90] 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

[87] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0194+0+DOC+XML+V0//EN

[88] *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).

[89] See http://www.infowar-monitor.net/2010/08/korea-trying-to-put-cybersecurity-on-g20-agenda/

[90] See http://ec.europa.eu/information_society/policy/nis/docs/comm_ciip/comm_en.pdf.

values, for Internet resilience and stability, in the framework of our strategic dialogue and cooperation with third countries and international organisations."

- In April 2009, the EU held a Ministerial Conference on Critical Information Infrastructure Protection (CIIP).[91]

- The Organization of American States has undertaken a number of steps to enhance cyber-security and improve regional responses to cybercrime.[92]

- One structure in Europe for improving coordination is the European Network and Information Security Agency (ENISA), founded in 2004.[93] 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.

- Recently a group of governmental experts from 15 countries agreed on a set of recommendations on cyber-security.[94]

All of these recent examples raise important questions, including: 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?

### B. 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?

[91] See http://www.tallinnciip.eu/doc/discussion_paper_-_tallinn_ciip_conference.pdf.

[92] See http://www.oas.org/juridico/english/cyber.htm.

[93] http://www.enisa.europa.eu/.

[94] See, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," United Nations A/65/201, July 30, 2010 and http://www.nytimes.com/2010/07/17/world/17cyber.html?_r=1

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 Cyber-security Initiative (CNCI) developed by the U.S.[95]  It is important to note that most elements of the U.S. plan focus on getting the federal government's own cyber-security house in order. The U.S. 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. Another example is the European Programme for Critical Infrastructure Protection set forth in a Directive EU COM(2006) 786, which obliges all Member States to adopt the components of the Programme into their national statutes. The Programme also applied to the European Economic Area.[96]

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.

## V. Recommendations for a way forward

Having set the stage in Sections I and II, provided an overview of substantive issues of cyber-security in Section III, and briefly outlined some international and national responses in Section IV, this Section proposes some additional thoughts for advancing the evolution of the international legal enabling environment for cyber-security.

It is recognized, of course, that there are existing mechanisms and instruments of international cooperation on legal issues of cyber-security of which the Council of Europe's Budapest convention is primary among them.  In this article the authors suggest three main ideas towards an evolving international best practice legal approach to cyber-security:  first, an approach that deconstructs matters of cyber security; second, an approach that looks at issues of cyber-security in a modular way; and third that these deconstructionist and modular approaches would provide a new lens through which to look at how to enhance future international cooperation and collaboration.

[95] *See*, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

[96]*See*, http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf.

Part of the deconstruction and modular approach advocated here is aimed at clarifying what exactly is meant by use of the catch-all phrase, “cyber-security.” Cyber-security does not necessarily mean cyber crime, which does not necessarily mean cyber-war. Threats to cyber security come from a number of sources, including, outdated legal architecture that doesn't necessarily reflect or apply well to the Internet, a dissonance of policy and legislative approaches by countries that make international collaboration and cooperation on certain levels difficult. In addition “buggy code,” bad practice and simple human error, as well as natural disasters can thwart such efforts and contribute to cyber insecurity.

So, going forward, what can be done to approach these new issues of cooperation? Firstly, it is suggested that policy-makers and legislators adopt at the same time a more modular and a layered approach to the many complex and often intertwined questions of cyber-security. Deconstruction begins by recognizing the manifold layers affected and tailoring security approaches to each layer. Those layers could include the infrastructure layer, the protocol or software layer, and the applications layer. In addition, a more resilient-based approach is emerging as the bell-weather instead of a “perimeter” security approach. Finally, a better and more realistic understanding of the incentives of the different actors involved is required, including economic incentives and personal incentives. Institutionally, attention needs to be paid to building capacity, especially for law enforcement personnel and harnessing the expertise of the private sector and other industry players at the various levels through engagement with the private sector, possibly through innovative public-private partnership mechanisms.

In analyzing and addressing the complex, multidimensional tapestry of international cyber-security legal issues, following is a synthesis of factors to be taken into consideration:[97]

- *Deconstructionalist (Layered) approach*. Cyber-security is not a monolith and responses to cyber-threats do not come in a “one-size-fits-all” package. Rather, the analysis of threats to cyber-security as well as the responses to them need to be looked at both in a deconstructed and modular 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 security 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.* Many tools, instruments and good practices are already available to help societies cope with cybercrime, including the Budapest Convention, but these need to be fully implemented and applied.

[97] This list of factors is derived from the discussion of the panelists at the Workshop. For details of the discussion that gave rise to this synthetic list, *see*, e.g., the Transcript referred to in supra footnote 6.

- *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 are three areas meriting attention:  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.