THE POTENTIAL FOR AN INTERNATIONAL LEGAL APPROACH TO CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

David Satola*
William J. Luddy, Jr.**

ABSTRACT: This article reviews a wide range of global efforts (and their limitations) to achieve cyber security (security of critical information infrastructure) through cross-border collaboration in both the private and public sectors, involving technologists, lawyers, and business process managers. The importance of cyber security extends beyond any government's legitimate concern for national security. There are significant interrelationships between terrorism, cybercrime, economic and human development, critical infrastructure protection, network security, regulatory reform, and Internet governance.

Technology and the legal and policy rationales behind its use on a global level, for both the public and private sectors, are the starting points for a fuller understanding of the work undertaken both domestically and internationally to provide "homeland security." The analysis is intended to raise awareness and posit the need for further international cooperation, coordination, and collaboration focusing on the legal aspects of critical information infrastructure protection that implicate and are affected by technology in the field.

CITATION: David Satola and William J. Luddy, Jr., The Potential for an International Legal Approach to Critical Information Infrastructure Protection, 47 Jurimetrics J. 315–333.

---

*Senior Counsel, the World Bank. The opinions expressed herein are those of the author and do not necessarily reflect those of the World Bank, its Board of Executive Directors, or its members.

**Clinical Professor, Rensselaer Polytechnic Institute, Lally School of Management and Technology.

I. BACKGROUND AND INTRODUCTION

This article examines the international legal aspects of critical infrastructure [1] protection (CIP), in particular, protection of critical information infrastructure (CII). In simple terms, the recommendation of many CIP *players* that more international cooperation is required in the area of CIP has been accepted.[2] But how is this cooperation to manifest itself? What are the current issues under discussion and is there a need for a wider international dialogue? To the extent that dialogue is already happening internationally, what opportunities present themselves for further dialogue and what criteria should be applied in assessing international CIP fora?

This article focuses on what is (and what is not) happening on the international stage with respect to the development of international legal regime for CIP.[3] In that sense, this article serves a dual purpose: (i) it alerts practitioners of developments internationally; and (ii) it argues in favor of the benefits of an international dialogue involving the range of stakeholders on key international legal aspects of CIP cooperation and coordination. Security of CII and CIP is a necessary prerequisite for ensuring good governance and empowering users and service providers alike by enhancing trust and confidence in the infrastructure and services that flow over it. This should be of particular relevance to practitioners and advisors of multinational enterprises or enterprises with international partners, vendors-suppliers, contractors, or customers.

---

1. "Critical infrastructure" and "critical infrastructure protection" can be broadly defined. As used in this article, critical infrastructure borrows from the definition found in the *Commission Green Paper on a European Programme for Critical Infrastructure Protection*, at 6–7, COM (2005) 576 final (Nov. 17, 2005) [hereinafter *Green Paper*], and used in the Council Framework Decision, Attacks Against Information Systems, 2005/222/JHA, 2005 O.J. (L 69) 67 (EU) [hereinafter Council Decision] of February 24, 2005. 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, at 20. 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 . . . ." *Id.*, Annex 1, at 19. 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 devices, 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." Council Decision, art. 1, at 68 The *CIIP Handbook* defines critical infrastructure as 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." 1 ISABELLE ABELE-WIGERT & MYRIAM DUNN, INTERNATIONAL CIIP HANDBOOK 25 (2006) [hereinafter CIIP HANDBOOK].

2. As noted in a recent World Bank study, "the challenges in responding to a new generation of cyber risks are more complex and require novel cross-border cooperation among governments, NGOs and private-sector entities . . . ." ROBERT BRUCE ET AL., WORLD BANK GROUP, CYBER SECURITY: A NEW MODEL FOR PROTECTING THE NETWORK 8 (2006) [hereinafter WORLD BANK I].

3. This article will not examine in any detail the international aspects (that is, the extraterritorial application) of existing U.S. homeland security law affecting CIP. These issues are covered in Jody R. Westby, *Countering Terrorism with Cyber Security*, 47 JURIMETRICS J. 297 (2007).

Increasingly, these enterprises and their legal advisors are confronted with a myriad of legal and regulatory compliance requirements with respect to CIP.[4] Notwithstanding the seeming proliferation of compliance requirements, these same enterprises and advisors are also becoming increasingly aware that mere compliance may not be sufficient to obtain the level of security or protection for CII that is necessary to meet all operational or business process purposes.

Today over 200 countries are connected to the Internet, which is undeniably a key element of the world's CII. And a key feature of the Internet is its distributed nature, which makes it a flexible and scalable tool. In part for these reasons, only a decade after its introduction into society, the Internet has increasingly become the primary tool of economic organization. The enterprises connected to the global economy are ever more dependent on technologies to support critical infrastructures and deliver essential services. But access is a double-edged sword. Increased access through technology is accompanied by attendant increases in cybercrime, penetrations, and disruptions that result in corruption, destruction of data, and denials of service (for example, phishing and spam), as well as other antisocial behaviors.

The importance of cyber security extends beyond any government's legitimate concern for national security. There are significant interrelationships between terrorism, cybercrime, economic and human development, critical infrastructure protection, network security, regulatory reform, and Internet governance. In addition, "best practice" regarding CIP is evolving, with interests of divergent stakeholders being served in different fora. For example, governments are interested in national security, 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. There are even different vocabularies emerging that support different interest groups and their respective subject matter mandates.[5]

The technology backbone on which today's economic activity depends demonstrates the critically intertwined nature of global business processes with CII. Yet critical infrastructure policy, law, and regulation are lagging,

4. *See generally* Thomas J. Smedinghoff, *Where We're Headed: New Developments and Trends in the Law of Information Security*, 3 PRIVACY & DATA SECURITY L.J. 103, 103–04 (2007). Smedinghoff provides an overview of U.S. law and observes three emerging trends applicable to CIP—a duty to provide security, the creation of "legal standard" for security based on security processes, and a duty to warn of security breaches.

5. For example, the term "information security" connotes a focus on the security of the content (data or information) and perhaps the storage medium but not necessarily the infrastructure over which it flows; "infrastructure security" seems to concern itself only with the hardware and not necessarily the content. Nevertheless, the two terms are often used interchangeably.

even in the most advanced countries.[6] Given the increasing dependence on "open network" technologies, the support, maintenance, and regulation of these global business processes and the infrastructures over which they flow have become interdependent on what had previously been perceived as discrete sectors—technological infrastructure, financial services, and law, for example. This sector-specific, "proprietary" approach in a world dominated by converged technologies is increasingly anachronistic. Fragmentation also occurs because institutional approaches and leveraging global experience on these issues is constrained by an ad hoc approach. As noted in a recent World Bank study: "the challenges in responding to a new generation of cyber risks are more complex and require novel cross-border cooperation among governments, NGOs and private-sector entities . . . ."[7]

At the first phase of the United Nations-sponsored World Summit on Information Society (WSIS) in December 2003, the international community endorsed a set of principles and an action plan that explicitly recognized the need for governments to create trustworthy, transparent, and nondiscriminatory legal, regulatory, and policy environments to maximize the social, economic, and environmental benefits of the Information Society.[8] The WSIS Action Plan also explicitly called for the promotion of a global culture of cyber security aimed at enhancing user confidence, building trust, and protecting both data and network integrity; addressing existing and potential threats to ICTs;[9] and taking up other information security and network security issues. This has been buttressed by the Organisation for Economic Co-operation and Development's (OECD's) Culture of Security guidelines[10] and the U.N. Resolutions on Cyber Security.[11]

---

6. Other articles in this Symposium provide important dimensions on these technology and law issues. *See, e.g.*, Michael Greenberger, *Teaching New Dogs Old Tricks: Reshaping the Department of Homeland Security's Technology Development Infrastructure*, 47 JURIMETRICS J. 281 (2007); Lucy L. Thomson, *Critical Issues in Identity Management Challenges for Homeland Security*, 47 JURIMETRICS J. 335 (2007).

7. WORLD BANK I, *supra* note 2, at 8.

8. *See* World Summit on the Info. Soc'y [WSIS], *Declaration of Principles*, WSIS Doc. WSIS-03/GENEVA/DOC/4-E (Dec. 12, 2003); WSIS, *Plan of Action*, WSIS Doc. WSIS-03/GENEVA/DOC/5-E (Dec. 12, 2003).

9. ICT stands for Information and Communications Technologies. This is a phrase that is widely used outside the United States and that encompasses a somewhat broader definition than Information Technology (IT).

10. ORG. FOR ECON. CO-OPERATION & DEV. [OECD], OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS: TOWARDS A CULTURE OF SECURITY (2002), *available at* http://www.oecd.org/dataoecd/16/22/15582260.pdf [hereinafter OECD GUIDELINES]; *see also* OECD, *Background Report on the Future of the Internet*, OECD Doc. DSTI/ICCP(2006)11 (Sept. 13, 2006) [hereinafter OECD, *Background Report*].

11. *See, e.g.*, G.A. Res. 57/239, U.N. Doc. A/RES/57/239 (Jan. 31, 2003); G.A. Res. 56/121, U.N. Doc. A/RES/56/121 (Jan. 23, 2002); G.A. Res. 55/63, U.N. Doc. A/RES/55/63 (Jan. 22, 2001).

As derived from various international sources,[12] a consensus appears to be emerging regarding certain principles applicable to CIP. First, the primary objective is that any disruption to CII be "brief, infrequent, manageable, . . . isolated and minimally detrimental . . . ."[13] Second, a cookie-cutter type program of CIP is neither appropriate nor recommended. Instead, CIP should be dynamic and "process-oriented"[14] rather than deterministic; it needs to be tailor-made ("proportionate," to borrow the E.U. phraseology) around the enterprise, group of enterprises, or industry, and around the level of threat and risk; and it should involve a wide range of stakeholders (both public and private) working on multiple levels (local, national, regional, and international).

Part of this best practice is the recognition for broad-based, continuous consultation. However, in the absence of a cross-sectoral, comprehensive approach as advocated in this article, there may be a danger that as the practice of each interest or stakeholder group evolves, divergences (silos) will occur thus undermining the consultative process.[15] Accordingly, this article provides an analysis of a number of different international initiatives, organizations, and fora with a view towards distilling their key attributes that could be used as the basis for further collaboration.

Continuous consultation is certainly a key part of avoiding an eventual "culture clash" between technologists and policy makers. Most CIP happens through Computer Emergency Response Teams (CERTs) which are mainly technologists operating at the national level. 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 that could 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 to CIP.[16] As is already recognized by the literature, coordination, collaboration, and consultation are key. The authors agree. But the answers to the questions of how, when, and where this coordination, collaboration, and consultation should take place and among whom they need to occur are not obvious. There is no single existing forum that has all the attributes to bring this about, so the question becomes: does the stakeholder community take an existing forum and make it work, or should a wholly new one be proposed (which has major implications for already stretched resources and fracturing of focus)?

---

12. *See generally, e.g.*, *Green Paper*, *supra* note 1; OECD GUIDELINES, *supra* note 10; CIIP HANDBOOK, *supra* note 1; WORLD BANK I, *supra* note 2.

13. *Green Paper*, *supra* note 1, at 1.

14. *See generally* Smedinghoff, *supra* note 4, at 113-14 (discussing what is entailed in process-oriented approaches).

15. This may also result in gradations in the development of technological-protection measures on the international level that create vulnerabilities (or weak links) in overall CIP technologies.

16. This phenomenon was noted with respect to cybercrime legislation by the European Union in the Council Framework Decision on Attacks Against Information Systems. Council Decision, *supra* note 1, at 67–68.

II. CRITICAL INFORMATION INFRASTRUCTURE PROTECTION IN CONTEXT

Critical information infrastructure protection (CIIP) (sometimes referred to as cyber security) is not an issue that can be approached in isolation from the other aspects of the CIP-enabling environment. Network security is affected by a mosaic of factors: different types of technology used in the infrastructure and services provided, different business processes and operational needs served by the network, other infrastructure, different user requirements, and different market and other incentives (including legal and regulatory) for security. An enabling environment that includes responses to these issues exists around this mosaic of factors. This enabling environment itself comprises an amalgam of policy, legal, market, technological, and other considerations that interact at the domestic and international levels.[17] Most CIP work is currently done through CERTs at the national level.[18] However, CERTs typically focus on technical issues and their main function is information sharing to provide primarily early warning functions.

Most countries have a patchwork of legal elements relating to this enabling environment. These elements address such issues as user authentication (for example, e-signature or digital-signature laws relating to e-commerce), data privacy protection, data retention, criminal or civil penalties against improper use of communications infrastructure (for example, cybercrimes and telecommunications legislation), and protections of intellectual property. But these national legal frameworks vary widely both in terms of the substantive issues covered and their content. Some countries and regions have specific legal means for addressing CIIP (for example, requirements in the European Union);[19] but many other countries have no specific legal provisions regarding CIIP.

Even where countries do have specific provisions dealing with CIIP, differences exist between countries as to how CII is to be protected. In some cases, CIIP is dealt with mainly through the application of industry norms or standards, such as functions provided by ICANN (the Internet Corporation for

---

17. Boutheina Guermazi & David Satola, *Creating the "Right" Enabling Environment for ICT*, *in* GLOBAL INFO. & COMMC'N TECHS. DEP'T, WORLD BANK GROUP, E-DEVELOPMENT: FROM EXCITEMENT TO EFFECTIVENESS 23 (Robert Schware ed., 2005) [hereinafter WORLD BANK II]; William J. Luddy, Jr. & Peter W. Schroth, *The New UNCITRAL e-Commerce Convention in the Mosaic of Developing Global Legal Infrastructure*, *in* ACADEMY OF LEGAL STUDIES IN BUSINESS 2006 NATIONAL REFEREED PROCEEDINGS (Ernest W. King ed., 2006), *available at* http://www.alsb.org/proceedings/copyright/UNCITRAL_William_Luddy_Peter_Schroth.pdf.

18. CERTs are usually the first responders to cyber attacks. WORKING GROUP ON INTERNET GOVERNANCE, BACKGROUND REPORT 27–28 (2005), *available at* http://www.wgig.org/docs/BackgroundReport.pdf [hereinafter BACKGROUND REPORT]; *see also* WORLD BANK I, *supra* note 2, at 4 n.12.

19. *See generally* Press Release, European Comm'n, The European Programme for Critical Infrastructure Protection (EPCIP) (Dec. 12, 2006), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/06/477.

Assigned Names and Numbers) with respect to administration of the Internet's so-called "core resources"—domain name registration, Internet Protocol (IP) addresses, and oversight of the root server system.[20] Moreover, the enabling environment is found not only at the national level but also at regional and international levels.[21] Effective CIIP will need to evaluate how the different parts of the mosaic interplay at different levels and how they can be addressed through a coherent, holistic approach. However, as will be demonstrated, there is no single international forum that includes all stakeholders for a dialogue on CIIP.

Evolving practice in the legal-enabling environment of CIP shows a focus on telecommunications infrastructure protection regulatory requirements, digital authentication (e-signature laws, for example), digital privacy protection, and cybercrime legislation.[22] The emphasis has been increasingly on imposing enforcement through laws or licensing arrangements under the legal framework.[23]

III. THE INTERNATIONAL DIMENSION

At the international level, many of the elements of this mosaic affecting CIIP (intellectual property, trade, Internet core resources, and telecommunications infrastructure regulation, to name a few)[24] are already within the ambit of one or more international organizations that provide (or could provide) a forum for discussing CIIP issues related to their respective mandates).[25] The

---

20. Joint Project Agreement Between the U.S. Department of Commerce and the Internet Corporation for Assigned Names and Numbers (2006), http:// www.ntia.doc.gov/ntiahome/domainname/agreements/jpa/signedmou290906.pdf [hereinafter Joint Project Agreement].

21. David E. Satola, *Legal Aspects of Internet Governance Reform*, 12 INFO. POLITY (forthcoming July 2007).

22. OECD, *Background Report*, *supra* note 10, at 11–13.

23. *Id.*

24. Respectively, these elements represent the World Intellectual Property Organization (WIPO), World Trade Organization (WTO), U.N. Commission on International Trade Law (UNCITRAL) or U.N. Conference on Trade and Development (UNCTAD), the Internet Corporation of Assigned Names and Numbers (ICANN), and the International Telecommunication Union (ITU).

25. Of course, a thorough review of the breadth and depth of organizations and their respective activities is beyond the scope of this article. However, for a more complete survey, see generally SECTION OF SCI. & TECH. LAW, AM. BAR ASS'N, INTERNATIONAL GUIDE TO CYBER SECURITY (Jody R. Westby ed., 2004). In the context of evaluating a set of enabling environment issues affecting Internet governance similar to that proposed here, the United Nation's Working Group on Internet Governance (WGIG) undertook an assessment of the roles and responsibilities of existing international forums. This assessment can be found in BACKGROUND REPORT, *supra* note 18. The *Background Report* "mapped" a range of Internet governance issues to institutions and assessed what the governance mechanisms of those institutions were, whether the institutions were inclusive (that is, open to a range of stakeholders participating in their deliberations), the extent to which the institutions had any executory power, and the extent of coordination of institutions with others with a similar mandate. *See generally id.* More information about the WGIG can be found at Working Group on Internet Governance, http://www.wgig.org (last visited May 22, 2007).

CIIP Handbook is emerging as a leading survey of the activities of different countries and organizations in the area of CIP and is updated periodically. The United Nation's Working Group on Internet Governance (WGIG) also surveyed different organizations' activities in the area of network security, but from the perspective of Internet governance.[26] For example, WIPO is the international forum for discussion of intellectual property issues and the likely forum for discussion of those issues as they relate to CIIP. But as will be shown, in some cases, where it would be expected that an organization or institution would be a likely forum for such discussions, this is not yet taking place; and, as noted by the WGIG, "*there are no international or intergovernmental organizations that have specific responsibility for coordinating global . . . activities* [*over cybersecurity*]."[27] And, where these discussions are taking place, they are either not inclusive enough (because of membership restrictions of the organizations) or not comprehensive enough (because of the limitations of the subject matter mandates of the organizations). The efficacy with which certain institutions address CIIP is measured against the principle of openness and inclusiveness of the range of stakeholders. Following is a brief survey of some of those organizations and institutions and how they are addressing CIIP. In the area of CIIP, each of these has a specific subject matter mandate and each has different membership or participation requirements and limitations.

A. Technical and Standards Bodies

Since the CII itself is comprised of various technological elements of hardware and software, it is probably axiomatic that standards are the starting point in the CIP discussion. Ironically, almost, technology and standards allow the interconnection and interoperability of different information systems, and technology and standards are also at the front line of ensuring CIP. It is therefore clear that access to these standards, as well as participation in their development, are necessary prerequisites to facilitate coordination and collaboration.[28] And, as is well known, technology is both an enabler of security and the first path down which threats to CII travel. Because the technology is itself, at the same time, part of the solution and part of the problem, the international assessment starts with the technology. A number of key organizations involved in technologies and standards operating at the international level follow.

---

26. BACKGROUND REPORT, *supra* note 18, at 19–33. The list of entities provided here is illustrative and not exhaustive. Among the institutions and organizations dealing with CIP issues surveyed in the *Background Report* are ICANN, the Internet Engineering Task Force (IETF), Organization of Economic Cooperation and Development (OECD), Council of Europe (CoE), the European Union, and the ITU.

27. *Id.* at 27.

28. BERKMAN CTR. FOR INTERNET & SOC'Y, HARVARD LAW SCH., ROADMAP FOR OPEN ICT ECOSYSTEMS 10–11, 21–26 (2005), *available at* http://cyber.law.harvard.edu/epolicy/roadmap.pdf.

1. *Forum of Incident Response and Security Teams (FIRST)*

The Forum of Incident Response and Security Teams (FIRST) is an international organization bringing together a number of national CERTs.[29] 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.

2. *Internet Corporation for Assigned Names and Numbers (ICANN)*

ICANN maintains the stability and security of the Internet, and therefore much of the information infrastructure. ICANN has been going through a transformation over recent years and is attempting to be more open and inclusive, as well as more international in its makeup at both the board level and the Government Advisory Committee (GAC) level. However, its role in administration of the Internet's core resources was recently reaffirmed in the updated agreement between ICANN and the U.S. Department of Commerce.[30] While ICANN does have convening ability and appeals to a wide range of stakeholders, it has a limited mandate with respect to CIP.

3. *Internet Engineering Task Force (IETF)*

The Internet Engineering Task Force (IETF) is, as its name suggests, mainly a technical organization that advises on and oversees various aspects of the technologies and protocols that make the Internet work.[31] While an open organization, its membership is mainly from technology and engineering backgrounds. Its work covers a range of technical issues relating to the security and stability of Internet infrastructure.

4. *International Organization for Standardization (ISO)*

The International Organization for Standardization (ISO) is comprised mainly of national standards bodies.[32] The ISO covers a wide range of standards including those related generally to basic information infrastructure operation and interoperability (for example, information technology and telecommunications systems) as well as specifically to CIP.

---

29. *See generally* FIRST – improving security together, http://www.first.org (last visited May 22, 2007).

30. Joint Project Agreement, *supra* note 20.

31. IETF Home Page, http://www.ietf.org (last visited May 22, 2007).

32. ISO – International Organization for Standardization (May 11, 2007), http://www.iso.org /iso/en/ISOOnline.frontpage. Membership in ISO is limited to one recognized national standards body per country. ISO membership also includes "correspondent" and observer groups.

5. *Private Sector*

In addition to the ISO, a number of private or industry associations and standards-setting bodies are involved in CIP. Examples include the Organization for the Advancement of Structured Information Standards (OASIS)[33] and the Jericho Forum of the Open Group,[34] to name a couple (both are fee-paying membership organizations). OASIS, a not-for-profit consortium, deals mainly with e-business standards. The Jericho Forum focuses on standards for network-security architecture CIP issues.

B. International Organizations

1. *International Telecommunication Union (ITU)*

Certainly, when viewing the work of its technical divisions—namely the Radiocommunication Sector (ITU-R) and the Telecommunication Standardization Sector (ITU-T)—the International Telecommunication Union (ITU) could be seen as a standards organization. But ITU has a number of initiatives regarding CIP including not only workshops and colloquia on issues such as spam and network security but also its mandate from WSIS to hold meetings on the so-called WSIS action line items.[35] Under the WSIS Action Plan, the ITU is charged with conducting consultations on, among other things, advancing cooperation at the international level, encouraging cooperation between governments and the private sector regarding cybercrime, and promoting appropriate legislation.[36] In connection with this activity, the ITU has initiated its Partnerships for Global Cybersecurity, which includes work programs in legal frameworks as well as watch, warning, and incident response.[37] The legal-frameworks program is examining the harmonization of legal frameworks, mainly in the area of cybercrime.[38] The ITU-sponsored action line consultations are more or less open meetings, requiring only registration.

---

33. OASIS, http://www.oasis-open.org/home/index.php (last visited May 22, 2007).

34. Jericho Forum, http://www.opengroup.org/jericho (last visited May 22, 2007).

35. The November 2005 *Tunis Agenda for the Information Society*, the main summit declaration of the second phase of the WSIS, provides for the ITU to undertake consultations on, among other things, network security and the "enabling environment." *See* World Summit on the Info. Soc'y [WSIS], *Tunis Agenda for the Information Society*, Annex & ¶ 108, WSIS Doc. WSIS-05/TUNIS/DOC/6(Rev.1)-E (Nov. 18, 2005) [hereinafter *Tunis Agenda*]; s*ee also* WSIS, *Plan of Action*, *supra* note 8, at C5.

36. *See* WSIS, *Plan of Action*, *supra* note 8, at C5 (entitled "Building Confidence and Security in the Use of ICTs").

37. *See* WSIS Action Line C5: Partnerships for Global Cybersecurity, http://www.itu.int/osg/spu/cybersecurity/pgc/index.phtml (last visited May22, 2007).

38. The Global Cybersecurity Gateway – Legislation and Enforcement, http://www.itu.int/cybersecurity/laws_legislation.html (last visited May 22, 2007).

Hamadoun Toure, incoming Secretary General of the ITU, confirmed the ITU's role in Internet governance in an interview published on January 12, 2007: "[ITU] will be focusing on cyber-security . . . ."[39]

2. *Organization for Economic Cooperation and Development (OECD)*

The Organization for Economic Cooperation and Development (OECD) has produced one of the foundational reference works in the area of CIP: *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*.[40] While the *OECD Guidelines* are available to all, participation in OECD proceedings is limited to its membership.[41]

3. *United Nations Commission on International Trade Law (UNCITRAL)*

The United Nations Commission on International Trade Law (UNCITRAL), established by the General Assembly, is the core legal body of the United Nations in the field of international trade law.[42] The Commission itself is composed of sixty member States elected by the General Assembly. "The Secretariat of UNCITRAL is the International Trade Law Division of the Office of Legal Affairs of the United Nations Secretariat."[43] UNCITRAL has produced a variety of texts including international conventions, model laws, and legislative guidelines (as well as several nonlegislative texts).[44]

In addition to UNCITRAL's substantial work in a variety of legal fields related to international commercial law,[45] the confluence of international trade and the "digital era" of electronic commerce since the early 1990s prompted the Commission to undertake a work program within its Working Group IV (WG IV) aimed at harmonizing global e-Commerce law and reducing the

---

39. *Internet Should Be Run by Key Players: New ITU Boss*, REUTERS, Jan. 15, 2007, http://www.reuters.com/article/internetNews/idUSL1291053820070115.

40. OECD GUIDELINES, *supra* note 10; *see also* ORG. FOR ECON. CO-OPERATION & DEV., THE PROMOTION OF A CULTURE OF SECURITY FOR INFORMATION SYSTEMS AND NETWORKS IN OECD COUNTRIES (2005), *available at* http://www.oecd.org/dataoecd/16/27/35884541.pdf [hereinafter OECD SURVEY].

41. The OECD describes its organization, in part, as "30 member countries sharing a commitment to democratic government and the market economy." OECD Home:About, http://www.oecd.org/about/0,2337,en_2649_201185_1_1_1_1_1,00.html (last visited May 22, 2007).

42. FAQ – Origin, Mandate and Composition of UNCITRAL, http://www.uncitral.org/uncitral/en/about/origin_faq.html (last visited May 22, 2007).

43. *Id.*

44. FAQ – UNCITRAL Texts, http://www.uncitral.org/uncitral/en/uncitral_texts_faq.html (last visited May 22, 2007).

45. UNCITRAL has completed work in the areas of international commercial arbitration, the international sale of goods, insolvency, international payments, the international transport of goods, electronic commerce procurement and infrastructure development, penalties, and damages. Work Carried Out by UNCITRAL, http://www.uncitral.org/uncitral/en/about/work.html (last visited May 22, 2007).

barriers to e-Commerce through several texts. Notably, these are UNCITRAL's Model Law on Electronic Commerce,[46] its Model Law on Electronic Signatures,[47] and most recently the Convention on the Use of Electronic Communications in International Contracts (e-Contracting Convention). The U.N. General Assembly adopted this Convention in 2004.[48] As a result of these efforts, WG IV and the UNCITRAL Secretariat have developed substantial policy and practical expertise in the commercial law aspects of a variety of issues related to CIIP.

An interesting and important attribute of UNCITRAL's working groups is the inclusiveness of a wide variety of stakeholders.

> In addition to member States, all States that are not members of the Commission, as well as interested international organizations, [including nongovernmental organizations (NGOs),] are invited to attend sessions of the Commission and of its working groups as observers. Observers are permitted to participate in discussions at sessions of the Commission and its working groups to the same extent as members.[49]

Further, UNCITRAL has an important convening power, engaging relevant and interested stakeholders[50] in its work.

UNCITRAL's success in this approach has been often demonstrated. For example, in its most recent work, the e-Contracting Convention, WG IV brought together member and Observer States, and a wide array of NGOs to undertake a broad assessment of national and sectoral issues related to global e-commerce. It then debated the best way to address the array of existing trade instruments that could be affected by electronic commerce and decided to address the emerging and evolving general principles of global e-commerce through an "umbrella" international text, the e-Contracting Convention.[51] Both the process (consultative and inclusive) and the product (a hopefully "future"-proof international instrument embodying general principles of good practice) are instructive when analyzing which potential forum is most desirable for taking up CIP legal issues.

Other useful examples (at least in terms of examples of a product) are UNCITRAL's Legislative Guide on Privately Financed Infrastructure Projects published in 2000 by the Working Group on Procurement (WG I) and its Legislative Guide on Insolvency Law published in 2004 by the Working

---

46. G.A. Res. 51/162, U.N. Doc. A/RES/51/162 (Jan. 30, 1997). with additional art. 5bis adopted by UNCITRAL, June 1998.

47. G.A. Res. 56/80, U.N. Doc. A/RES/56/80 (Jan. 24, 2002). It should be noted that versions of this Model Law have been promulgated in only four countries, while its Model Law on Electronic Commerce is more widely adopted.

48. G.A. Res. 60/21, Annex, U.N. Doc. A/RES/60/21/Annex (Nov. 23, 2005).

49. Methods of Work, http://www.uncitral.org/uncitral/en/about/methods.html (last visited May 22, 2007).

50. It might be noted that nongovernmental organizations (NGOs) must be accredited to participate.

51. G.A. Res. 60/21, s*upra* note 48, Annex.

Group on Insolvency (WG V). [52] The Legislative Guides are a different kind of product from the e-Contracting Convention or the two model laws developed by WG IV. However, this demonstrates the flexibility inherent in UNCITRAL products to meet various needs. One could envisage a set of generally applicable CIP legal principles from the highly effective process environment already embedded in UNCITRAL's working methods.

Although ordinarily considered in an international commercial law context, UNCITRAL reviewed a series of legal topics for possible future work that are related to legal issues noted in this paper at its July 2006 Plenary Session.[53] Issues such as cross-border authentication, liability and standards of conduct for ISPs, privacy and data protection, spam and cybercrime, among others, were reviewed.[54] It is interesting to note that the UNCITRAL Secretariat observed with respect to several of these topics that "[l]ack of appropriate rules, guidelines or voluntary codes of conduct, or even the perception of insufficient legal protection, undermine confidence in electronic commerce and constitute an obstacle to its development."[55] Additionally, and related to the issues raised in this paper, UNCITRAL convened a Colloquium on International Commercial Fraud in April 2004.[56] In its Report on the Colloquium,[57] the UNCITRAL Secretariat noted suggestions for further work in this field that the Commission might wish to undertake.[58] It is possible, therefore, that UNCITRAL, given its competence, expertise, working methods, and prominence, could provide a forum for examination of various important issues related to CIP, perhaps in collaboration with other specialized organizations.

52. *See, e.g.*, 2004 – UNCITRAL Legislative Guide on Insolvency Law, http://www.uncitral.org/uncitral/en/uncitral_texts/insolvency/2004Guide.html (last visited May 22, 2007).

53. U.N. Comm'n on Int'l Trade Law [UNCITRAL], *Note by the Secretariat: Possible Future Work in the Area of Electronic Commerce*, U.N. Doc. A/CN.9/604 (May 9, 2006).

54. *Id.* ¶¶ 7–24, 47–52, 61–62.

55. *Id.* ¶ 50.

56. *See* UNCITRAL Colloquium on International Commercial Fraud, April 14–16, 2004, *Draft Programme*, *available at* http://www.uncitral.org/pdf/english/news/fraud-program-e.pdf.

57. UNCITRAL Colloquium on International Commercial Fraud, April 14–16, 2004, *Note by the Secretariat: Report on UNCITRAL Colloquium on International Commercial Fraud*, U.N. Doc. A/CN.9/555 (May 19, 2004).

58. *Id.* ¶¶ 62–71. In particular, the Secretariat noted that "[i]t may also be possible to consider a regulatory regime that could govern conduct in situations where, for example, a fraudster misuses a web site to defraud its victims and law enforcement agencies seek to have an Internet service provider shut down that web site." *Id.* ¶ 71.

4. *United Nations Economic Commission for Europe (UNECE)*

The Centre for Trade Facilitation and Electronic Business [59] (UN/CEFACT) is a United Nations body organized within the United Nations Economic Commission for Europe (UNECE). It is actively engaged in a wide range of projects related to international trade and, in particular, creating the technical frameworks for electronic commerce between countries. There is considerable emphasis in its work on the use of information and communications technologies to help harmonize the processes, procedures and information flows that may contribute to the growth of global commerce.[60]

UN/CEFACT's largely technical work programs result in the development of "Recommendations" that may be adopted, where appropriate, by government agencies and private sector organizations.[61] It seeks to bring together and create collaborations between governments and private business that "secure the interoperability for the exchange of information between the public and private sector."[62] Its mission statement states: "[UN/CEFACT's] principal focus is on facilitating national and international transactions, through the simplification and harmonisation of processes, procedures and information flows, and so contribute to the growth of global commerce."[63]

As a standards development body, UN/CEFACT works with other standards development organizations (such as the ISO and OASIS, mentioned above) as well as international bodies such as UNCITRAL, the World Trade Organization, and the World Bank. Technologists from around the world representing private companies, government agencies, and other organizations participate directly on its technical development projects.[64] And to the extent that there may be legal issues to be addressed, the UN/CEFACT Legal Group provides assistance to the technical groups.

---

59. *See generally* United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) – UNECE (May 11, 2007), http://www.unece.org/cefact.

60. U.N. Econ. & Soc. Council [ECOSOC], U.N. Ctr. for Trade Facilitation & Elec. Bus. [UN/CEFACT], *Mandate, Terms of Reference and Procedures for UN/CEFACT*, U.N. Doc. TRADE/R.650/Rev.4 (Apr. 25, 2005). UN/CEFACT's mandate is described therein as follows:

> Trade facilitation mechanisms, other commercial and governmental business processes and electronic business standards are vital factors in the development of world trade and, therefore, central to the remit of the United Nations Economic Commission for Europe (UNECE). The UNECE, which acts as the focal point within the United Nations for these matters, established UN/CEFACT with the mandate to achieve improved worldwide coordination and cooperation in these areas. The Centre is mandated to develop and undertake a programme of work of global relevance that meets current and future demands as required by its mission.

Id. ¶ 2.

61. *See* UNITED NATIONS, ECONOMIC COMMISSION FOR EUROPE, SUMMARY OF UN/CEFACT TRADE FACILITATION RECOMMENDATIONS, U.N. Doc. ECE/TRADE/346 (2006).

62. United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) – UNECE (Mar. 3, 2006), http://www.unece.org/cefact/about.htm.

63. *Id.*

64. Participants work as volunteers and may or may not be supported by their own organizations.

5. *World Bank*

The World Bank is active in the area of CIP (both in CII and in connection with communications infrastructure used in the financial sector) primarily through the financing and related advisory services it provides in connection with its project-lending work. This is done mainly on a project- and sector-specific, country-by-country basis. Global best practice is evidenced, however, in World Bank publications dealing with CIP.[65]

C. Other International Initiatives

More recently, however, the Internet Governance Forum (IGF) has emerged as a potential candidate forum for a broad-based, multi-stakeholder, comprehensive international forum for a holistic discussion of CIP.[66] The IGF, consistent with its mandate, has no executory power, and is intended, rather, as an open, transparent and inclusive forum for a broad range of stakeholders for the exchange of ideas about topics of interest to the broader Internet community. These features are what make the IGF a potentially attractive model for CIP consultation.

The first meeting of the IGF was held in Athens, Greece, from October 30 to November 2, 2006. Among the four main themes of the Athens meeting of the IGF was a session dedicated to "Security" that focused on a broad range of issues affecting the stability and security of the Internet.[67] In addition to the main session on Security, a number of parallel workshops at the IGF also explored different aspects of network security in the Internet context.[68] The legal workshop recognized the distributed, nonhierarchical nature of the Internet was itself reflected in a dynamic legal-enabling environment for Internet

65. These publications include, among other things, WORLD BANK I, *supra* note 2; GEORGE SADOWSKY ET AL., WORLD BANK, INFORMATION TECHNOLOGY SECURITY HANDBOOK (2003), and the related Web site: InfoDev World Bank, http://www.infodev-security.net (last visited May 23, 2007); and in the financial sector Thomas C. Glaessner et al., *Electronic Safety and Soundness: Securing Finance in a New Age* (World Bank, Working Paper No. 26, 2004). See also CIIP HANDBOOK, *supra* note 1, at 379–81, for an overview discussion of the World Bank's different activities in these areas.

66. The IGF was one of the concrete results of the Tunis phase of WSIS. The mandate for the IGF is contained in the *Tunis Agenda*, *supra* note 35, ¶ 72. More information about the IGF is available at The Internet Governance Forum (IGF), http://www.intgovforum.org (last visited May 23, 2007).

67. Transcript from Internet Governance Forum "Security" Panel, Athens, Greece (Oct. 31, 2006), http://www.intgovforum.org/IGF-Panel3-311006.txt.

68. Among the workshops exploring different aspects of security were ones dealing with spam, *see* Inaugural Meeting of the IGF, Oct. 30–Nov. 2, 2006, Athens, Greece, *Workshop: Anti-Spam Toolkit* (Nov. 1, 2006), http://www.intgovforum.org/Athens_workshops/Workshop%20report%20SPAM.pdf, protecting Internet infrastructure, *see* Inaugural Meeting of the IGF, Oct. 30–Nov. 2, 2006, Athens, Greece, *Workshop: Infrastructure Security* (Oct. 31, 2006), http://www.intgovforum.org/Athens_workshops/Internet%20Infrastructure%20Security%20Workshop%20report.pdf, and legal issues of Internet Governance, *see* Inaugural Meeting of the IGF, Oct. 30–Nov. 2, 2006, Athens, Greece, *Workshop: Legal Aspects* (Nov. 1, 2006), http://www.intgovforum.org/Athens_workshops/IGF%20Workshop%20report%20Legal%20Aspects.pdf.

Governance. Indeed, the IGF legal workshop focused on the relationship between legislative or judicial decisions at the national level and the development of international legal norms, as well as the effect that actions at the international level have on the evolution of national laws. Network security is perhaps the best example of this distributed dynamic in the enabling environment.

Another interesting development arising out of the inaugural IGF was the formation of so-called "Dynamic Coalitions" dealing with a number of thematic issues, including one dealing with spam.[69] One of the key elements of the IGF is its open, broad-based, multi-stakeholder, inclusive, and consultative approach. Both the attention of the international community in the preparation for and attendance at the inaugural IGF (including the emergence of the Dynamic Coalitions) are a testament to the convening power that the IGF has.

With two important caveats,[70] the open nature of the IGF and its convening power augur in favor of the IGF, or something with attributes similar to it, serving as a candidate for an international forum for a broad-based dialogue on CIP.

D. Regional Organizations and Initiatives

A number of regional groups are also looking at the issue of CIP. In addition to the Council of Europe, which has already been discussed, above, the European Union stands out in its efforts to address CIIP as a regional priority.

1. *Council of Europe (CoE)*

The Council of Europe (CoE) has promulgated its cybercrime convention.[71] The convention addresses cybercrimes of data interception, data interference, system interference, and illegal access, as well as other crimes that are facilitated by computers. Notwithstanding its many positive features, the convention has come under criticism for being overly broad[72] and dependent

69. See Dynamic Coalitions, http://www.intgovforum.org/Dynamic%20Coalitions.php (last visited May 23, 2007), for a list of the Dynamic Coalitions and brief descriptions of their focuses. The Dynamic Coalitions, while they came together in connection with the IGF, are independent of the IGF and demonstrate the convening power of the IGF.

70. These caveats are: (i) whether the convening power of the IGF can be sustained over time and (ii) the limited mandate of the IGF focusing on matters related to Internet governance (even though this mandated can be interpreted more broadly under the *Tunis Agenda*, *supra* note 35, to include all ICT-related issues).

71. Council of Europe, Convention on Cybercrime, CETS No. 185 (Aug. 5, 2006), http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. The Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, CETS No. 189 (Jan. 28, 2003), is available at http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm.

72. Under the Cybercrime Convention, for example, sending an email without prior authorization could be construed as a crime, that is, accessing a computer "without right."

on a fairly sophisticated supporting legal infrastructure.[73] The convention is drafted broadly enough that its scope could arguably extend beyond just computer-related crimes. In addition, while a "regional" initiative in Europe, the CoE can invite (and has invited) non-European countries to accede to the convention, and a number have accepted.[74]

2. *European Union*

The European Union has for many years had a number of directives dealing with different aspects of CII, including data privacy protection, anti-spam, and protections against attacks on information systems, as well as a number of related issues such as digital authentication.[75] In addition, it has issued a public consultation Green Paper, *On a European Programme for Critical Infrastructure Protection*, concerning a European approach to CIP.[76]

IV. THE WAY FORWARD

There is no disagreement about the complexity of attaining true security through CIP. There is also no denying the increasing role that the law and legal frameworks (regional, national, and international) are playing in this mix—although a sustainable CIP approach could never rest solely on law and legislation. It is clear that vigilant assessment and improvement of existing regulatory tools, the development of legal enforcement tools, and on-going coordination of CIP efforts is required to meet an ever expanding and sophisticated threat.

As mentioned above, most work in CIP is currently done at the national level through CERTs. One of the implicit conclusions of the Background Report was that current international structures are inadequate to deal comprehensively with CIP but could provide a platform for further consultation and coordination. The encouragement for further international coordination and collaboration is also underscored by the OECD, in the WSIS, and the World Bank.

---

73. *See* SADOWSKY ET AL., *supra* note 65, at 178–79. *See generally* Satola, *supra* note 21. The Cybercrime Convention requires signatories to have in place adequate procedural safeguards for official access to computers for investigative purposes.

74. As of May 23, 2007, nineteen States have ratified the Convention, including the United States (one of four nonmember States that had signed the Convention). Council of Europe, Convention on Cybercrime, CETS No. 185, Status (May 23, 2007), http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT= 185&CM=&DF=&CL=ENG.

75. Council Directive 2002/58/EC, Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37 (EC); Council Directive 1999/93/EC, Community Framework for Electronic Signatures, 2000 O.J. (L 13) 12 (EC); Council Directive 95/466/EC, Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (EC); *Commission Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC*, COM (2005) 438 final (Sept. 21, 2005).

76. *Green Paper*, *supra* note 1.

CII is a distributed infrastructure. This distributed aspect is reflected in its users, services providers, owner–operators, and regulators. Because of the diverse interests represented in the different stakeholder groups already involved in CIP, effective multi-stakeholder international consultation will have to accommodate the full range of stakeholders, who sometimes may have divergent points of view (for example, privacy advocates and national security interests).

Attributes that would support effective international dialogue on these issues, as they emerge from this survey, include openness to and inclusiveness of participants (to ensure the range of interest groups are represented), credibility (whether established through process or methodology or through the product), flexibility, and convening power. It appears that neither the formality nor the executory power of the forum are requirements.

Despite their contributions to and interest in the area of CIP, it would nonetheless appear that with a few possible exceptions, none of the organizations, institutions, or forums surveyed in this article (either because of the inherent limitations in their membership or mandate) would really emerge as potential candidates for a broad-based, inclusive, multi-stakeholder, comprehensive, international forum for a holistic discussion of CIP legal issues. The two exceptions are (1) the Internet Governance Forum (IGF), based on its convening power, multi-stakeholder appeal, and open and consultative attributes and (2) UNCITRAL, also based on its convening power as well as its past experience and flexibility in adapting outputs to needs.

Based on the organizations, institutions, and fora surveyed, and based on attributes necessary to support a holistic dialogue, it appears that the options for further international dialogue are some variation of the following three items. First, continue with the status quo (that is, make use of existing fora or organizations.) As noted earlier, however, the current status quo may be insufficient to meet the need for more international collaboration in the CIIP domain.

A second option is to design a new forum for these purposes. However, such a forum would require resources for organization and may diminish the effectiveness of the already scarce resources of participants who now participate in another forum or event. Following the example of UNCITRAL's WG IV in preparing the e-Contracting Convention or its WG I and V in their Legislative Guides, we could consider promulgation of an international instrument setting forth a statement of principles.

A third option would be to promote the emergence of a Dynamic Coalition on CIIP issues. Such efforts might be coordinated by UNCITRAL, but another organization that focuses on the technology of CIP, such as UN/CEFACT, would actually develop the appropriate legal and technological infrastructures. UNCITRAL does have experience collaborating with other organizations where its primary competence, international commercial law, is implicated. And it seems clear from the foregoing discussion that the important issues in CIIP affect the commercial legal infrastructure.

We have sought in this review to examine a different but no less important aspect of "homeland security." It has broader and global implications for a secure CII environment that can support the critically important and immediate interests of homeland and global security and suggests an approach to develop an international legal infrastructure that promotes long-term stability in trade and development as well.