SCHOOL OF LAW
CASE WESTERN RESERVE UNIVERSITY

Canada-United States Law Journal

Volume 37 | Issue 2 Article 10

January 2012

# International Governance Framework for Cybersecurity, The

Paul Rosenzweig

CANADA-UNITED STATES LAW JOURNAL · VOLUME 37 · ISSUE 2 · 2012

# THE INTERNATIONAL GOVERNANCE FRAMEWORK FOR CYBERSECURITY

*By: Paul Rosenzweig*[*]

Cyberspace is a domain without distinct borders where action at a distance is a new reality. In effect, almost every computer in America is a potential border entry point. This reality makes international engagement on cybersecurity essential.

Even more notably, the sheer scale of the network demands a global approach. The Internet is as large a human enterprise as has ever been created. More than 2 billion users[1] send more than 88 quadrillion emails annually, and they register a new domain name with the Internet Corporation for Assigning Names and Numbers ("ICANN") every second of every day.[2] The scope of the Internet is as broad as the globe and that makes the scope of the Internet governance question equally as broad – who sets the rules for the Internet and what rules they set is a fundamental question that can only be answered on an international basis.

This then, is a fundamental question–perhaps *the* fundamental question–of cyber conflict today: How does a fractured international community respond to the phenomenon of the Internet?

One has the clear sense that, forty years ago, when the Internet was born,[3] the various sovereign nations of the world did not think much about the innovation. By and large, they systematically ignored it and let it grow on its own with a relatively unstructured set of governing authorities. And then sometime in the last ten years, the nations of the world looked up and suddenly recognized that the Internet had become this immense entity and that it had a vast influence and power. The Internet could be used to change governments and spread culture; it could run nuclear power plants

---

* Professorial Lecturer in Law, George Washington University; Principal, Red Branch Consulting, PLLC; Visiting Fellow, The Heritage Foundation. This work will appear as a chapter in the forthcoming book *Cyber Warfare: How Conflict in Cyberspace is Challenging America and Changing the World* (Praeger 2012). 

1. *E.g.,* Jonathan Lynn, *Internet Users to Exceed 2 Billion This Year*, REUTERS (Oct. 19, 2010, 9:21 AM), http://www.reuters.com/article/2010/10/19/us-telecoms-internet-idUSTRE69I24720101019.

2. Barry Riholtz, *60 Seconds: Things that Happen Every 60 Seconds*, THE BIG PICTURE (Dec. 26, 2011, 6:00 AM), http://www.ritholtz.com/blog/2011/12/60-seconds-things-that-happen-every-sixty-seconds/.

3. Phillip Rosenbaum, *Web Pioneer Recalls 'Birth of the Internet'*, CNN TECH (Oct. 29, 2009), http://articles.cnn.com/2009-10-29/tech/kleinrock.internet_1_internet-leonard-kleinrock-computer?_s=PM:TECH.

and fight a war. With that realization, sovereign nations became quickly and intensely interested in the Internet. The result is a trend toward the "re-sovereignization"[4] of cyberspace or what Chris Demchack and Peter Dombrowski of the Naval War College call the "Rise of a Cybered Westphalian Age"[5] – that is, an age in which sovereign nations control the Internet.[6]

And so, the questions are: Who will run the Internet? Will it be separate sovereign countries? Will it be the UN? Or a set of non-governmental organizations like ICANN and the Internet Engineering Task Force ("IETF")? Or, perhaps a series of bi-national or multilateral groups? For America this question poses a problem. Some think it is critical that our engagement occur in a manner that is protective of American interests and maintains American freedom of action.[7] By contrast, some (including the Obama Administration) advocate a general approach that favors the development of multilateral norms to preserve the openness of the Internet,[8] while relying on supra-national organizations to manage cybersecurity

4. *National Security Experts Discuss Need for Cybersecurity Cooperation*, ABA NOW AROUND THE BAR (Aug. 5, 2012), http://www.abanow.org/2012/08/national-security-experts-discuss-need-for-cybersecurity-cooperation/ (discussing Rosenzweig's comments about the U.N.'s proposed changes in the governing of the internet). *Compare* Scott Cleland, *Twitter's RealPolitik & the Sovereign-ization of the Internet*, FORBES (Jan. 27, 2012, 6:03 PM), http://www.forbes.com/sites/scottcleland/2012/01/27/twitters-realpolitik-the-sovereign-ization-of-the-internet/ (discussing Twitter's ability to censor content from users in specific countries allowing countries to maintain sovereignty within their geographic borders in cyberspace), *with* Omar El Akkad, *Google Threatens to Pull Out of China*, GLOBE & MAIL, http://www.theglobeandmail.com/technology/google-threatens-to-pull-out-of-china/article 1207172/ (last updated Aug. 23, 2012) (discussing Google's plans to stop censoring search results within China's geographic borders).

5. Chris Demchack & Peter Dombrowski, *Rise of a Cybered Westphalian Age*, 5 STRATEGIC STUDIES Q. 32 (2011).

6. In 1648, the Peace of Westphalia ended the 30 Year War and established the modern system of national sovereignty. The Westphalian system is premised on the territoriality of states, and the principle of non-interference by one state in the internal affairs of another. That system has, more or less, controlled international affairs for over 450 years. *See* Peace of Westphalia Treaty, May 15–Oct. 24, 1648, 30 I.L.M. 2.

7. *See* Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, HOOVER INST., Feb. 2011, at 12 (arguing that no treaty which is beneficial to the United States will be adopted by other countries).

8. *See* THE WHITEHOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE 20 (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf ("International norms are critical to establishing a secure and thriving digital infrastructure.").

problems.[9] The choice is of truly profound significance–perhaps more so than any other policy question to be addressed in the cyber domain.

This brief article begins by describing the existing Internet governance and describing the dynamic that is leading to change. After assessing some of the barriers to effective international Internet governance, it closes with a brief discussion of United States-Canada cybersecurity cooperation.

## I. EXISTING INTERNET GOVERNANCE STRUCTURES AND CHANGING INTERNATIONAL NORMS

In this first section, I want to briefly describe the existing Internet governance structures using the security of the domain name system as a prism through which to examine their operation. I then want to examine how nation states are responding to that governance structure and close with concerns expressed by human rights activists.

### *A. ICANN and the IETF*

Domain names are familiar to everyone who uses the Internet. In any web address (for example, http://www.redbranchconsulting.com) it is the portion of the address after http://www. Domain names are familiar ways to identify the web page you are seeking to access or the email address you are trying to reach. We know them and recognize them readily–Microsoft.com takes you to Bill Gates' company[10] and direct.gov.uk takes you to the front page of Her Majesty's Government in London.[11]

Of course, computers do not use names like "Microsoft" or "Her Majesty's Government" to route traffic. They use numbers. The Domain Name System ("DNS") is, in effect, a translation system–it takes a domain name and translates it to an Internet Protocol address ("IP address").[12] The IP address is a binary number inside the computer (that is, just a string of 1s and 0s), but it is usually written in a traditional format when put down for humans to read (for example 172.16.254.1).[13] The IP address tells the Internet routing

9. *See id.* at 21-22 (discussing multinational organizations that address cybersecurity policies and activities).

10. MICROSOFT, http://www.microsoft.com (last visited Oct. 7, 2012).

11. GOV'T OF THE U.K., http://direct.gov.uk (last visited Oct. 7, 2012).

12. *See* Bradley Mitchell, *DNS-Domain Name System*, ABOUT.COM GUIDE, http://compnetworking.about.com/cs/domainnamesystem/g/bldef_dns.htm (last visited Oct. 7, 2012) ("DNS automatically converts the names we type in our Web browser address bar to the IP addresses of Web servers hosting those sites.").

13. *See, e.g.*, Bradley Mitchell, *IP Address*, ABOUT.COM GUIDE, http://compnetworking.about.com/od/workingwithipaddresses/g/ip-

system where a particular server is on the Internet, and then the Internet Protocol tells the system how to get the message from "here" to "there," wherever "there" may be.[14]

So the DNS link works in a three-stage process. An individual (Paul Rosenzweig) registers a domain name (redbranchconsulting.com) which is hosted on a server somewhere and that server is identified by an IP address. When a potential client wants to access the Red Branch web site by typing in that domain name, the DNS programming helps to route the request to the right server and return the web page.

The addressing function of the DNS is absolutely critical. If the DNS system were corrupted, hijacked or broken, then communications across the Internet would break down. And it also means that keeping a good registry of which domain names are in use is just as vital. If "Microsoft.com" is taken by Microsoft, the computer software giant, it cannot be used by Microsoft a (hypothetical) manufacturer of small soft washcloths. *Somebody* needs to be in charge of keeping the books and making sure they are all straight.

That *somebody* is the Internet Corporation for Assigning Names and Numbers ("ICANN").[15] ICANN is a non-profit organization that sets the rules for creating and distributing domain names.[16] When the Internet was first turned on, the function for assigning names was actually done by a single man, John Postel,[17] who helped create the first Internet as a project for the Advanced Research Projects Administration ("ARPA").[18] Since ARPA was a Federal government

addresses.htm (last visited Oct. 7, 2012) (An IP address is a binary number that uniquely identifies computers..."). *See also* Bradley Mitchell, *Introduction to the Domain Name System (DNS)*, ABOUT.COM GUIDE, http://compnetworking.about.com/od/dns_domainnamesystem/a/ introduction-to-dns_domain-name-system.htm (last visited Oct.7, 2012) (discussing how binary code is translated into a traditional format).

14. *See* Mitchell, *supra* note 12.

15. *See generally Welcome*, ICANN, http://www.icann.org/en/about/welcome (last visited Oct. 7, 2012) (explaining that "coordinates the Domain Name System (DNS), Internet Protocol (IP) addresses, space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions.").

16. *Definition of ICANN*, ICANN, http://www.icann.org/en/about/learning/glossary/i?language=%2A%2A%2ACURRENT_LANGUAGE%2A%2A%2A (last visited Oct. 7, 2012).

17. *See* PGMedia, Inc. v. Network Solutions, Inc., 51 F. Supp. 2d. 389, 391 (D.N.Y. 1999).

18. *See id.*

funded agency this, in effect, meant that the U.S. government handled the naming function.[19]

In the long run, of course, as the Internet grew to span the globe, a U.S.-run and –managed naming convention was considered too insular and unilateral.[20] ICANN was chartered in 1998 as a means of transitioning control over Internet naming from the U.S. government to a non-profit private sector organization.[21] Today, ICANN operates from California but has a global constituency, registering new domain names every day.[22]

In theory, the DNS system should be completely transparent – knowing a domain name (the "cyber-persona" of a person or company) you should be able find out who the real person behind the domain name is. Unfortunately, the system does not work as effectively as it should. In December 2011, ICANN completed a comprehensive review of the WHOIS functions.[23] The conclusion of the report is both chilling and accurate. The report "concisely present[s] in a balanced and fair manner the very real truth that the current [WHOIS] system is broken and needs to be repaired."[24] Because domain registry companies (like GoDaddy[25]) accept identification that appears to be lawful and because they make no real attempt to verify the information they receive, the WHOIS registry is littered with errors, both accidental and deliberate.[26]

Just as ICANN is the international organization that runs the program for assigning domain names, another non-governmental

19. *See generally id.* (explaining that Postel's project was through a contract between DARPA, ARPA, and UCLA).

20. *See* Tony Bradley, *The Upside of Unbinding ICANN from U.S. Oversight*, PCWORLD (Oct. 1, 2009), https://www.pcworld.com/businesscenter/article/172954/the_upside_of_unbinding_icann_from_us_oversight.html.

21. *See* ICANN, *supra* note 15.

22. *See* Esther Dyson, *Internet Corporation for Assigned Names and Numbers (ICANN): The Short Version*, 11 WORLD TRADE & ARB. MATERIALS 32, 39-40 (1999) (explaining that four different constituency groups represent communities around the globe and that ICANN operates out of Los Angeles, California).

23. *See generally* WHOIS POLICY REVIEW TEAM, FINAL REPORT TO ICANN (2012) (stating that all of the meetings of the review team occurred during 2011).

24. *Id.* at 6.

25. *See id.* at 29 (stating that GoDaddy is one of the largest domain registry companies).

26. *See id.* at 32 (stating that registrar companies are "required to verify information at the time of registration but in practicality it does not happen"); *see also id.* at 73 (explaining that accidental errors often occur because buyers do not realize how important the information is).

organization, the Internet Engineering Task Force ("IETF"), is responsible (in an indirect way) for developing the technical aspects of the computer code and protocols that drive the Internet.[27] Nobody actually owns or operates the Internet itself. While private sector and government actors own pieces of the cyber domain (various routers and nodes, for example) the actual rules for how the cyber domain works are set by the IETF which is an "open international community of network designers, operators, vendors and researchers concerned with the evolution of the Internet architectures and the smooth operation of the Internet."[28] This community operates by the promulgation of technical standards, which, in the end, become *de facto* operating requirements for any activity in cyberspace.[29] Thus, some questions about cybersecurity necessarily require engagement with an engineering community that is both internationalist and consensus-oriented, characteristics that may be inconsistent with effective U.S. government action.

Put another way, the IETF's self-described mission is to "make the Internet work better"[30] but it quickly notes that it is an "engineering" group so what it means by "better" is "more technically effective," not better in some metaphysical sense.[31]

The IETF is a self-organized group of engineers who consider technical specifications for the Internet.[32] Anyone may join and the group's proposals (or decision not to make a proposal) are the product of a rough consensus.[33] The IETF has no enforcement function at all –

27. *See generally Overview of the IETF*, INTERNET ENGINEERING TASK FORCE, http://www.ietf.org/old/2009/overview.html (last visited Oct. 20, 2012) (explaining the organizational hierarchy of the IETF).

28. *Id.*

29. INTERNET ENGINEERING TASK FORCE, http://www.ietf.org (last visited Oct. 20, 2012).

30. Paul Rosenzweig, *The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY, 245, 255 n.44 (2010).

31. *See Getting Started in the IETF*, INTERNET ENGINEERING TASK FORCE, http://www.ietf.org/newcomers.html (last visited Oct. 20, 2012) ("make the Internet work better from an engineering point of view").

32. *See* Paul Hoffman, ed., *The Tao of IEFT: A Novice's Guide to the Internet Engineering Task Force*, INTERNET ENGINEERING TASK FORCE, https://www.ietf.org/tao.html (last modified Nov. 2, 2011) ("The IETF is a loosely self-organized group of people who contribute to the engineering and evolution of Internet technologies. It is the principal body engaged in the development of new Internet standard specifications.").

33. *See id.* (explaining that in order to join, a person subscribes to the mailing list as well as defining "rough consensus" as "a very large majority of those who care agree").

anyone is free to disregard the technical standards it sets, but they do so at their own peril.[34] Because of the openness, inclusiveness, and non-partisan nature of its endeavors, IETF standards have become the "gold standard" for Internet engineering.[35] In addition to the standard setting function, IETF also identifies lesser standards, known as "best current practices," that are more in the nature of good advice than of operative requirements.[36] Given the near-universality of IETF standards and practices, anyone who chooses not to follow the standards set forth risks ineffective connections to the broader network. And so, even without a single means of forcing people to follow its dictates, the IETF in effect sets the rules of the road for the Internet technical functions.[37]

By way of example, one of the recent technical specifications adopted by the IETF is something known as "DNSSEC," which stands for Domain Name System Security Extension.[38] Under the general rubric of DNSSEC, the IETF has proposed a suite of security add-on functionalities that would become part of the accepted Internet Protocol.[39] The new security features would allow a user to confirm the origin authentication of DNS data, authenticate the denial or existence of a domain name, and assure the data integrity of the DNS.[40] In other words, the DNSSEC protocols would allow users to be sure that when they attempt to connect to a domain name (say "whitehouse.gov") they are reaching the "true" whitehouse.gov web site and not some phony facsimile of that web site.

34. *Id.* ("The IETF makes voluntary standards that are often adopted by Internet users, but it does not control, or even patrol, the Internet.").

35. *Id.* ("The IETF is not a traditional standards organization, although many specifications that are produced become standards.").

36. *See id.* (explaining that "best current practices" (BCPs) make recommendations for the current applications on the internet).

37. *See generally* INTERNET ENGINEERING TASK FORCE, *supra* note 29 (explaining that the function of the IETF is to make the Internet run smoothly by recommending a series of technical functions for those who wish to follow them).

38. *See generally* R. Arends, et al., *DNS Security Introduction and Requirements*, INTERNET ENGINEERING TASK FORCE (Mar. 2005), http://www.ietf.org/rfc/rfc4033.txt (explaining extensions to the Domain Name System to protect data integrity).

39. *See id.* at 6 (explaining the proposed security add-ons and what their purposes are); *see also DNSSEC - What Is It and Why Is It Important?*, ICANN, http://www.icann.org/en/about/learning/factsheets/dnssec-qaa-09oct08-en.htm (last visited Oct. 21, 2012) (explaining what the DNSSEC does and what its implementation into Internet Protocol would mean for users.)

40. *See generally* Arends, *supra* note 38 (explaining the process that the security add-on functionalities go through in order to secure data with in DNS).

Without that sort of security system, efforts to navigate the web are susceptible to "man-in-the-middle" attacks – an attack where the malicious actor steps into the middle of a conversation and hijacks it by making independent connections with the victims. From the middle vantage point, he can relay messages between the victims making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the malicious actor.[41]

To see the interplay between IETF and ICAAN, consider the question of how DNSSEC will be implemented. Critical to DNSSEC's effective functioning is the need to establish a "chain of trust" for domain name authentication.[42] After all, how do you know that the "chase.com" web page is authentic? Because a certificating authority (probably a company, like VeriSign,[43] that is in the business of authentication) has distributed to Chase an authentication key. And how do you know that VeriSign is itself, authentic? At some point up the chain there has to be an "original" root authentication that serves as a "trust anchor" to the chain of trust. Currently, the trust anchor is provided by ICANN; though, some people do not trust ICANN because it is an American company and is thought to still be subservient to American interests.

And so, the international régime of NGO Internet governance works, pretty effectively, but there are some who doubt its true neutrality.[44] This has led sovereign nations to think of ways to reassert their authority.

### *B. The Rise of Sovereigns*

Nobody owns the Internet. As we have said, currently technical standards are set by the IETF and limited substantive regulation of the Internet (e.g. the creation of new top level domain names and the

41. Paul Rosenzweig, *Online Piracy and Internet Security: Congress Asks the Right Question but Offers the Wrong Answers*, HERITAGE FOUND. (Jan.17, 2012), http://www.heritage.org/research/reports/2012/01/online-piracy-sopa-and-internet-security-pipa-bills-in-congress.

42. *See generally* Goldsmith, *supra* note 6 (explaining the process of what happens in DNSSEC verification of domain names).

43. *See generally* VERISIGN, http://www.verisigninc.com/?loc=en_US (last visited Nov. 1, 2012) (detailing the services offered by VeriSign).

44. *See generally ICANN*, CHEMISTRY DAILY, http://www.chemistrydaily.com/chemistry/ ICANN (last visited Nov. 1, 2012); *see also* Sam, *ICANN*, THE WEB WORD, http://classes.dma.ucla.edu/Winter06/161B/projects/lenny/final/articles/show/10 (last visited Jan. 1, 2013) (discussing personal views of respective writers).

like) is done by ICANN.[45] This quasi-independent non-profit international governance is the current norm.[46]

On a nation-state level, this is slowly changing. Some countries have responded to this reality by attempting to cut themselves off from the Internet or censor traffic arriving at their cyber borders. The most notorious example is China's attempt to construct a "Great Firewall" to keep Internet traffic out of the country.[47] China conducts an active effort to suppress adverse news on the Internet, with more than 300,000 Internet monitors engaged in the process.[48] As a result the recent unrest in the Middle East seems to be unable to find traction in China. The instinct to regulate is not, however, limited to authoritarian régimes; even liberal Western countries like Australia have proposed restrictions on Internet traffic, albeit for facially more legitimate reasons, such as limiting the spread of child pornography.[49]

Or, consider another example from a relatively small nation, Belarus. According to the Library of Congress on December 21, 2011 the Republic of Belarus published Law No. 317-3.[50] The law imposes restrictions on visiting and/or using foreign websites by Belarusian citizens and residents.[51] It also requires that all companies and individuals who are registered as entrepreneurs in Belarus use only domestic Internet domains for providing online services, conducting sales, or exchanging email messages.[52] In addition, the owners and

45. *See generally* Hoffman, *supra* note 32 (describing the purpose of IETF in technical standards of the internet); *see also* ICANN, *supra* note 14 (describing regulation by ICANN of the internet).

46. *See* ICANN, *supra* note 14 (describing ICANN as a non-profit organization which operates outside of the United States Government); *see also* Hoffman, *supra* note 32 (describing IETF as a non-profit independent organization devoted to making the internet work better).

47. *See* THE GREAT FIREWALL OF CHINA, http://www.greatfirewallofchina.org/ (last visited Nov. 4, 2012) ("test any website and see real-time if it's censored in China").

48. *See* L. Gordon Crovits, *Opinion: Dictators and Internet Double Standards,* WALL ST. J. (Mar. 7, 2011), http://online.wsj.com/article/SB10001424052748703580004576180662638333004.html (describing the measures China takes to suppress news that may affect their government in a negative way).

49. *See Australia Says Web Blacklist Combats Child Porn*, ASSOCIATED PRESS (Mar. 27, 2009), http://phys.org/news157371619.html (discussing Australian proposed internet blacklist which has been created to combat child pornography).

50. *See* Peter Roudik, *Belarus:Browsing Foreign Websites a Misdemeanor*, LIBR. OF CONG. (Dec. 30, 2011), http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205402929_text.

51. *See id.* (discussing the law's purposes).

52. *Id.*

administrators of Internet cafés or other places that offer access to the Internet might be found guilty of violating this Law and fined and their businesses might be closed if users of Internet services provided by these places are found visiting websites located outside of Belarus and if such behavior of the clients was not properly identified, recorded, and reported to the authorities.[53] Talk about a Westphalian response to the borderless Internet!

The impetus for greater control also led a number of nations to call for a U.N. organization (the International Telecommunications Union ("ITU"), about which more will be discussed later) to exert greater control over the operation of the Internet.[54] Likewise, some nations have urged greater international control over the content of the Internet.[55] Indeed, Russia and China have begun advocating for the adoption of an international treaty to govern conflict in cyberspace – a Cyberspace Geneva Convention, if you will.[56] Critical to their draft proposals are the adoption of cyber conflict norms about targeting), married to an international standard that allows each nation to manage its domestic Internet however it pleases (in effect, giving international law approval to domestic Internet censorship).[57]

Indeed, according to Demchack and Dombrowski, this development is inevitable:

A new "cybered Westphalian age" is slowly emerging as state leaders organize to protect their citizens and economies individually and unwittingly initiate the path to borders in cyberspace. Not only are the major powers of China and the United States already

53. *Id.*

54. *See* Leo Kelion, *US Resists Control of Internet Passing to UN Agency*, BBC NEWS (Aug. 2, 2012), http://www.bbc.co.uk/news/technology-19106420 (discussing the opposition of the U.S. government to proposals which would allow the ITU to take greater control over the operation of the internet); *see also* Brendan Sasso, *House to Examine Plan for United Nations to Regulate the Internet*, THE HILL: HILLICON VALLEY (May 26, 2012), http://thehill.com/blogs/hillicon-valley/technology/229653-house-to-examine-plan-to-let-un-regulate-internet (explaining the proposal before the U.S. House of Representatives regarding turning control of the internet over to the UN's ITU).

55. *See* Sasso, *supra* note 54 (explaining that U.S. hesitates to turn control over to countries which "ban certain terms from search" because it would in turn take away from the freedom that the internet provides).

56. *See Russia Calls for Internet Revolution*, RUSSIA TODAY (May 28, 2012, 4:42 PM), http://rt.com/news/itu-internet-revolution-russia-386/ (explaining both the plan Russia proposed for greater international control as well as China and India's support for the proposal).

57. *See* G.A. Res. 66/359, 66th Sess., ¶¶ c & e, U.N. Doc. A/66/359 (Sept. 14, 2011) (stopping the proliferation of information which incites terrorism and other acts against a country and reaffirming a State's rights and responsibilities to protect themselves against such acts).

demonstrating key elements of emerging cybered territorial sovereignty, other nations are quickly beginning to show similar trends. From India to Sweden, nations are demanding control over what happens electronically in their territory, even if it is to or from the computers of their citizens.

This process may be meandering, but . . . it was inevitable, given the international system of states and consistent with the history of state formation and consolidation. As cyberspace is profoundly man-made, no impossible barriers hinder the growth of national borders in cyberspace. They are possible technologically, comfortable psychologically, and manage-able systemically and politically.[58]

That prospect certainly reflects the reality of the issue from the perspective of nations, but it may not reflect the intent of the broader Internet community. We can be sure of resistance to this trend.

### *C. Internet Access as a Human Right*

One way to think of that resistance is to ask: do human beings have a fundamental right to have access to the Internet? How you view the question may very well drive your assessment of the right structures for the international governance of the Internet. If you think access is a fundamental right, you will be unalterably opposed to the new cybered Westphalia.

Vinton G. Cerf thinks the answer is clearly "no," and he ought to know. [59] After all, Cerf is one of the "fathers of the Internet"[60] and currently serves as the "Chief Internet Evangelist" for Google—he is one of the grand old men of the network.[61] According to Cerf, the right way to think about technology is as an "enabler" of rights – not as the right itself.[62] Human rights "must be among the things we as humans need in order to lead healthy, meaningful lives, like freedom from torture or freedom of conscience. It is a mistake to place any particular technology in this exalted category, since over time we will end up valuing the wrong things."[63] After all, 150 years ago having a horse might have been an essential enabler; 50 years ago a car. The Internet, like any technology, is a means to an end, not the end itself.

---

58. DEMCHACK & DOMBROWSKI, *supra* note 5, at 35.

59. Vinton G. Cerf, *Internet Access is Not a Human Right*, N.Y. TIMES, Jan. 5, 2012, at A25.

60. If any endeavor that is barely forty years old can be said to have a "grand old man."

61. *Vincent G. Cerf: Vice President and Chief Internet Evangelist*, ICANN: BOARD, http://www.icann.org/en/groups/board/cerf.htm (last visited Jan. 1, 2013).

62. Cerf, *supra* note 59.

63. *Id.*

Others disagree. For example, the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression,[64] is of the view that a complete denial of access to the Internet is a violation of international law: "[C]utting off users from Internet access, regardless of the justification provided, [is] disproportionate and thus a violation of article 19, paragraph 3, of the International Covenant on Civil and Political Rights."[65] The Rapporteur views the denial of Internet access as an unacceptable means of controlling freedom of expression and limiting dissent.[66] Set against the backdrop of the Arab Spring,[67] there is a certain force to his concerns.

In the end, the disagreement may not matter. Most would admit that the Internet is an exceedingly powerful enabler of freedom. Those who design the Internet, and those who manage it, ought to do so cognizant of the great force they have unleashed – and that it can be used for good or ill. One way to think about the "Internet as human right" issue is to simply ask whether those designing the Internet's architecture (like the IETF) might not owe a duty of care to the general world population to take greater steps to make the Internet impervious to malware and viruses.

## II. CHALLENGES IN INTERNATIONAL INTERNET GOVERNANCE

In this section, I want to consider some successes (rare) and failures (sadly more frequent) that arise from our current international structures and look at some of the satisfying and less satisfying suggestions for improving the situation.

### *A. Cybercrime and The Russian Business Network*

The Russian Business Network ("RBN") is truly a child of the Internet – it could not really exist without it.[68]

64. *See generally* Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/17/27 (May 16, 2011) (by Frank LaRue).

65. *Id.* ¶ 78.

66. *Id.* ¶ 33.

67. *See* Crovits, *supra* note 48.

68. I learned a great deal about the Russian Business Network from and was pointed to some of the sources referenced in this section by a presentation given by Mr. Rob Wile, a graduate student in my Summer 2011 class at Medill School of Journalism, Northwestern University. *See also* Peter Warren, *Hunt for Russia's Web Criminals*, THE GUARDIAN (Nov. 14, 2007), http://www.guardian.co.uk/technology/2007 /nov/15/ news.crime (discussing the creation of the Russian Business Network by graduate students much like Google).

The RBN was an Internet service provider, run by criminals for criminals.[69] Its founding date is unclear but it may go back as far as 2004.[70] The RBN was allegedly created by "Flyman," a 20-something programmer who is said to be the nephew of a well-connected Russian politician.[71] Though its initial activity appears to have been legal it quickly morphed into something more. It provided domain names, dedicated servers, and software for criminals – a one stop shopping center for those who want to be active on the Internet.[72] The RBN is sometimes called a "bullet proof network" because, in effect, users are capable of hiding their criminal activity and are "bullet proof" against prosecution or discovery in their country of origin.[73]

To a large degree, the RBN was just another business: it offers access to "bulletproof" servers for $600/month as well as highly effective malware (price $380 per 1,000 targets),[74] and rents out botnets at the bargain basement price of $200 per bot.[75] All this comes with free technical support, patches, updates and fixes.[76] In its heyday, the RBN was responsible for some of the largest criminal hacks to date – one example would be the infamous "Rockfish" incident, in which users were tricked into entering personal banking

69. *See generally* Brian Krebbs, *Shadowy Russian Firm Seen as Conduit for Cybercrime*, WASH. POST (Oct. 13, 2007), http://www.washingtonpost.com/wpdyn/content/article/2007/10/12/AR2007101202461.html (explaining that RBN has strong links with Russian criminal underground as well as the government of Russia).

70. *See* Brian Krebs, *Mapping the Russian Business Network*, SECURITY FIX: BRIAN KREBS ON INTERNET SECURITY (Oct. 13, 2007, 12:02 AM), http://voices.washingtonpost.com/securityfix/2007/10/mapping_the_russian _business_n.html (analyzing the origins of RBN and many of the cybercrime attacks that they orchestrated).

71. *See* Warren, *supra* note 68 (describing the background of "Flyman" who supposedly turned RBN toward criminal activity).

72. *See* Krebbs, *supra* note 69 (describing the various crimes that RBN has protected including identity theft and child pornography).

73. *See* Krebbs, *supra* note 69 (describing bullet proof hosting as a web service that will remain reachable despite efforts by law enforcement to shut the site down).

74. Malware is short for "malicious software," in other words a software program that has a malevolent effect. *See* Krebbs, *supra* note 69 at 2 ("...a cyber-criminal who clears these hurdles can rent a dedicated Web site from the Russian Business Network for about $600 a month, or roughly 10 times the monthly fee for a regular dedicated Web site at most legitimate Internet companies").

75. Botnets are networks of controlled computers– short for a "robot network" because the innocent computers are controlled, like robots, by someone else. Sometimes, we also call the innocent computers "zombies" for much the same reason. *See* Warren, *supra* note 68.

76. *See* Warren, *supra* note 68.

information on the web resulting in losses in excess of $150 million.[77] In another incident, a keystroke logger program (one that records keystrokes input on a keyboard – like a password entry) was placed on the computers of most of the customers of the Bank of India.[78] The RBN is also said to have provided some support for Russia during the Georgian and Estonian conflicts.[79]

Under severe pressure from the Russian government, which was deeply embarrassed by some of the RBN's activities and subject to pressure from other countries, the RBN officially closed its doors in 2008[80]–though many suspect that rather than "closing" they simply moved offices to another location.[81] Still, it is encouraging to see that some forms of international cybercrime cooperation are possible.

### *B. The Limits of Internationalism*

Despite the success with using international pressure to disrupt the RBN, severe procedural difficulties limit the effectiveness of criminal law in addressing transnational cybercrime. Most American procedural criminal law requirements are premised on the assumption that the crimes to be investigated and prosecuted have occurred within the geographic boundaries of the United States.[82] In the rare cases where cybercrimes are geographically limited in this way, these procedural requirements are suitable. But the reality is that cybercrime is predominantly (and almost exclusively) transnational in character.

In many ways the situation is much like the challenge facing state law enforcement officials prosecuting Depression-era bank robberies. The perpetrators could escape investigation and prosecution simply by changing jurisdictions and hiding behind differing laws.[83] The problem is best exemplified by Clyde Barrow's famous fan letter to

77. See this story and others presented in the deeply detailed study of the RBN in VERISIGN IDEFENSE INTELLIGENCE OPERATIONS TEAM, THE RUSSIAN BUSINESS NETWORK: RISE AND FALL OF A CRIMINAL ISP 19 (2008).

78. *Id.* at 28.

79. John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES, Aug. 13, 2008, at A1.

80. VERISIGN IDEFENSE INTELLIGENCE OPERATIONS TEAM, *supra* note 77, at 32.

81. Warren, *supra* note 68.

82. United States v. Verdugo-Urquidez, 494 U.S. 259, 266 (1990) (holding that the 4th Amendment envisioned protects only searches conducted on U.S. soil).

83. *See* Paul Rosenzweig, *Cybersecurity and Public Goods: The Public/Private 'Partnership'*, HOOVER INST., Sept. 2011, at 19.

the Ford automobile company, thanking it for providing the means by which he and Bonnie escaped justice.[84]

The solution, of course, was to federalize the crime of bank robbery and, effectively, eliminate the boundary problem.[85] But what the U.S. government could do with the stroke of a Federal legislative pen takes years and years of work in the international context. Today we are just at the beginning of constructing a transnational set of procedural rules for cybercrime. For the most part, information sharing across national boundaries is slow and limited – far slower and more limited than the nimbleness with which criminals can change their tactics. Substantive convergence of the law is even further in the future and may well prove impossible.

To date the only effort to develop a unitary procedural approach to cybercrime is the Convention On Cybercrime developed by the Council of Europe.[86] It aspires to create a single set of cyber laws and procedures internationally in order to insure that there is no safe harbor for cybercriminals.[87] But the process is slow; only thirty-eight countries have ratified the Treaty in nine years.[88] And significant cultural and legal hurdles have further slowed convergence.[89] Thus, in the criminal domain the single most significant question is one of extraterritoriality and engendering cooperation from international partners.

The signatories to the Convention on Cybercrime (notably they do *not* include Russia and China) have agreed to pass common laws criminalizing cybercrime and to cooperate in the trans-border investigation of cyber incidents.[90] The trans-border efforts have, however, been hampered by adherence to out-dated modes of cooperation. Countries sharing cyber information must still proceed through Mutual Legal Assistance Treaties[91] and Letters Rogatory,[92] processes first developed in the 1800s.

84. Letter from Clyde Barrow to Henry Ford (Apr. 10, 1934) (on file with Ford Motor Museum ID: 64.167.285.3).

85. Robbery & Burglury, 18 U.S.C § 2113 (2002).

86. Convention on Cybercrime, Nov. 23, 2001, C.E.T.S. No. 185.

87. *Id.*

88. *Status of Convention*, COUNCIL OF EUR., http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (last updated Jan. 21, 2013).

89. Jeremy Kirk, *Despite Controversy, Cybercrime Treaty Endures*, CIO (Nov. 21, 2011), http://www.cio.com/article/694681/Despite_Controversy_Cybercrime_Treaty_Endures.

90. Convention on Cybercrime, *supra* note 86.

91. Amalie M. Weber, *The Council of Europe's Convention on Cybercrime*, 18 BERKELEY TECH. L.J. 425, 442 (2003) (discussing the purpose of MLATs).

The growing consensus, therefore, is that the Convention on Cybercrime does not work on at least two levels—operationally and strategically.[93] Operationally, the Convention's procedures are widely regarded as ineffective, slow, and cumbersome.[94] What is necessary, in the first instance, is an effort through the Council of Europe to adopt more rapid response mechanisms that work in real-time. The technology for such an effort is readily available in the current interconnected environment.

Reopening the treaty for modifications of this sort is likely to be a challenge, but one with a potentially significant long-term benefit. If that course were deemed inexpedient, perhaps a better option would be to act on a bilateral basis. Failing an effort to revise the Convention, the United States can and should negotiate bilaterally to achieve the same effect with a "coalition of the willing."[95]

Strategically, the absence of China and Russia from the Convention makes it a bit of a paper tiger. If they refuse to bind themselves to assist in the prosecution of cybercriminals they become, in effect, a safe haven. The international community needs to move beyond the current structure to a "naming and shaming" campaign modeled on that developed to combat money laundering by the Financial Action Task Force ("FATF").[96]

The FATF was created based on the recommendation of the G-7 back in 1989 and created a task force of experts in banking and law enforcement to create a set of recommendations for best practices in defending against illegal practices.[97] The FATF has moved beyond recommendations to a routine system of self-inspection.[98] More importantly, the FATF uses the same standards to publicly identify high-risk and non-cooperative jurisdictions that do not implement

92. Letters Rogatory Defined, 22 C.F.R. § 92.54 (2006).

93. Weber, *supra* note 91.

94. *See* Paul Rosenzweig, *Making Good Cybersecurity Law and Policy: How Can We Get Tasty Sausage?*, 8 J.L. & POL'Y FOR THE INFO. SOC'Y 389, 398 (2011).

95. Joseph Lester, *Remarks by Leonard S. Spector*, 99 AM. SOC'Y INT'L. L. PROC. 251 (2005).

96. *High Risk and Non-Cooperative Jurisdictions*, FINAL ACTION TASK FORCE, http://www.fatf-gafi.org/topics/high-riskandnon-cooperative-jurisdictions/more/aboutthenon-cooperativecountriesandterritoriesncct-initiative.html (last updated Aug. 23, 2012).

97. *Who We Are*, FINAL ACTION TASK FORCE, http://www.fatf-gafi.org/pages/aboutus/ (last visited Jan. 1, 2013).

98. *See* ORG. FOR SEC. & CO-OPERATION IN EUR. PERMANENT COUNCIL, DECISION NO. 487: FINANCIAL ACTION TASK FORCE (FATF) SELF ASSESSMENTS ON TERRORIST FINANCING (2002).

adequate safeguards.[99] Creating a similar Cybercrime Action Task Force ("CATF") should be a top priority for identifying and combating countries that serve as havens for bad actors.

### *C. Data Sovereignty*[100]

While cybercrime prevention is often a story of Western cooperation and non-Western intransigence, even the West cannot always find unity of purpose in its efforts. Indeed, the Westphalian image is one of conflict, rather than cooperation. Already we can see how it will play out in cyberspace. Consider first, the issue of data sovereignty: In a wide, interconnected world, data and applications run on servers. Those servers, though connected to a borderless web, all reside somewhere physically. Who controls them and the data they contain?

Today, these servers are situated based upon factors like weather (cooler is better), existing infrastructure, and proximity to data sources (to reduce time in transit). It may soon become more commonplace, however, to situate your data storage centers and servers based on legal concerns: "While the location of a data storage center may be irrelevant to many operations and applications, the physical location of a piece of data or information is often critical in determining which sovereign nation controls that data. If information is power, then the location of information may determine who exercises power in cyberspace."[101] The trend toward cloud systems – and the lack of any consensus on the rules that govern the data stored in them – is a paradigmatic example of the breakdown in international governance.

One area in which this breakdown is manifest is in the development of conflict around the issue of "data sovereignty," that is, the question of which sovereign controls the data. Increasingly, the cloud-structure of Internet service is allowing for distributed service models at a distance. Data "owned" by an American company, say, may be stored in Canada based on service provided by a French entity. The question of sovereignty is really just a question of jurisdiction and, therefore, of control and authority – but in a cyber-world where the geographic boundaries are indistinct those questions become quite ambiguous.

---

99. *See* FINAL ACTION TASK FORCE, *supra* note 96.

100. The following section is derived from Michael Chertoff, *Data Sovereignty in the Cloud: The Issues for Government*, SAFEGOV.COM (Nov. 1, 2011), http://safegov.org/2011/11/1/data-sovereignty-in-the-cloud-the-issues-for-government, to which the author of this article contributed in the drafting.

101. *Id.*

In short, the question is: "Whose law is to be applied? The law of the country where the customer created the data? The law of the country (or several countries) where the server(s) are maintained? Or the law of the home country where the data storage provider is headquartered? Or all of the above?"[102] The truth is that nobody really knows.

In an ideal world, we could at least hope that the international community would agree upon an international standard for the choice of law rules – in effect agreeing on the bare minimum of deciding what rules govern the question of how to decide which rules govern. But prospects for such an agreement are highly unlikely. No multinational organization (say, the United Nations) will undertake that sort of effort and even if it did we might not like the result.

Instead, disputes over data sovereignty and jurisdiction will have to be resolved one case at a time. The single factor that is likely to determine the resolution of each dispute is almost certainly going to be the physical location of the server. For example, when the United States recently began seeking banking data from Swiss banks for tax collection purposes, the critical factor was that economic considerations required the Swiss banks to have a physical presence in the United States. Without it they were not true international banks – but with it they were manifestly subject to American jurisdiction and control.[103] By contrast, when data is housed outside the United States it is much more likely that the other jurisdiction will be able to impose its own legal requirements on the data – almost as if data were subject to an *in rem* sort of action.

The bottom line however, is clear – there is a growing dispute over precisely whose law will apply to legal conflicts on the Internet. And in the end, in the absence of any systematic effort to construct a legal system that fosters dispute resolution, these sorts of questions are far more likely to be resolved by reference to the physical infrastructure of the network than to any other frame of reference. Where the servers are and where the data is stored will, in the end, likely control whose law applies. As they say, "geography is destiny."[104]

102. *Id.*

103. *Id.*

104. *Id.*

### *D. The Coming International Privacy War*[105]

There is another looming cloud on the Internet governance horizon that ought to be highlighted, a coming conflict between the privacy values of the United States and those of the European Union ("EU"). This conflict is best seen in a challenge to cloud-based data aggregation services – services that are generally accepted in the United States, but not in the EU.

Recently EU Justice Commissioner Vivian Redding stated, "[We] believe that companies who direct their services to European consumers should be subject to EU data protection laws. Otherwise, they should not be able to do business on our internal market."[106] In this vein the EU plans to back up new data privacy requirements with rules that fine businesses five percent of their global turnover if they breach the requirements.[107] Even more recently the Commission Nationale de L'informatique et des Libetes ("CNIL"), which is the data privacy authority of France, issued a report on behalf of all EU data protection authorities, critiquing Google, by name, for their inadequate privacy protections. According to the CNIL, Google's platform allowed the "uncontrolled combination of data across services" in violation of EU law.[108] The CNIL, as well, threatened to sue Google if it did not change its policy.

This is challenge, in the guise of privacy regulation, is really the same challenge just noted with regard to the question of data sovereignty – whose law applies? Where, earlier, we imagined disputes regarding data retention and commercial conflicts, now we can see that the same issues will bedevil more fundamental questions about the legality of existing Internet business models and the application of divergent domestic laws on privacy. These conflicting legal requirements will deter product development, and create legal ambiguity. If you want a particularly stark example of how this

105. This section is derived from Michael Chertoff, *Cloud Computing and the Looming Global Privacy Battle*, WASH. POST (Feb. 9, 2012), http://www.washingtonpost.com/opinions/cloud-computing-sets-stage-for-a-global-privacy-battle/2012/02/06/gIQAhV2V2Q_story.html, to which the author of this article contributed in the drafting.

106. Kevin J. O'Brien, *E.U. to Tighten Web Privacy Law, Risking Trans-Atlantic Dispute*, N.Y TIMES, Nov. 10, 2011, at B4.

107. Ravi Mandall, *New EU Date protection Laws May Impose Big Fines*, ITPROPORTAL.COM (Dec. 7, 2012), http://www.itproportal.com/2011/12/07/new-eu-data-protection-laws-may-impose-big-fines/.

108. *See Google's New Privacy Policy: Incomplete Information and Uncontrolled Combination of Data Across Services*, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (Oct. 16, 2012), http://www.cnil.fr/english/news-and-events/news/article/googles-new-privacy-policy-incomplete-information-and-uncontrolled-combination-of-data-across-ser/.

conflict might play out, consider that in September 2012 police in Brazil briefly detained the head of Google's local operations because the company had refused an order to take down a YouTube video. The video was about a paternity suit involving a local mayoral candidate.[109] In the end, Google complied – not in this case because of where the data was, but one suspects because of where their own manager was physically located – in a Brazilian jail.

We can only expect this problem to be exacerbated as time goes by. If choice of law rules for commercial disputes are beyond our expectations for the UN (or any other multinational body) how much more unlikely is it that rules regarding the regulation of content of the web can be developed for universal application. While the US-EU dispute is emblematic of the possibility for divergent viewpoints, lurking behind it are even more significant disputes. In the end, China's Great Firewall and Iran's plan to build a "halal" network are really efforts by sovereigns to control the substance of information on the network. Though the types of control they seek to exercise and the reasons they do so are be more problematic than the European privacy efforts they all, in the end, share the same typology – sovereign nations seeking to regulate content. In the absence of an international régime we would hope that the Western nations would agree on a joint position in opposition to content control. Unfortunately, it appears more likely that a "privacy war" will develop as the United States and the EU contest to impose their will. This is the worst possible result, pitting natural allies against each other.[110]

### *E. An International Strategy*

Given the limitations of a Westphalian-based policy, it is not surprising that the Obama Administration has pursued a multilateral approach to international cyber issues. The recently released *International Strategy for Cyberspace* points toward the creation of an "open, interoperable, secure, and reliable" communications and information architecture (surely a positive goal) through building and sustaining "norms of international behavior."[111] The strategy goes further in articulating the norms it seeks to foster (freedom, privacy, respect for property, protection from crime, and the right of self-defense)[112] but one may be forgiven in thinking that these norms are

109. *The World is What You Make It*, THE ECONOMIST, Oct 27, 2012, at 21.

110. Chertoff, *supra* note 105.

111. THE WHITEHOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD (2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

112. *See generally id* at 10.

articulated at too high a level of generality; and unlikely to find great acceptance in many nations that value neither privacy nor freedom.

The limits of this sort of strategy are best exemplified by how the strategy addresses the problem of cybercrime. We have seen, earlier, how limited the effectiveness of the Cybercrime Convention has been.[113] And yet the principal goal of the new strategy for addressing cybercrime is to "harmonize criminal law" internationally by "expanding accession" to the Convention.[114] If there were a realistic prospect that criminal havens, like Russia and China, would both join the convention and also implement it aggressively, this policy would likely be effective. But in the absence of that prospect, the promise of a multilateral policy seems a bit empty.

### *F. Cyber Warfare Convention*

Or consider how the multilateral impulse has begun to drive negotiations over a cyber-warfare convention. For years, the United States resisted Russian blandishments to begin negotiations over a cyber-warfare convention, akin to the chemical warfare convention.[115] The Russian model would outlaw certain types of cyber-attacks (say on civilian targets, like electric grids) as out of bounds.[116] At its core, this seems a reasonable objective.

The principal American objection has been that a cyber-treaty, unlike a ballistic missile treaty, is inherently unverifiable.[117] In other words, in a world where weapons cannot be identified and counted and where attribution is difficult, if not impossible, how could any country be assured that others were abiding by the terms of the agreement?

Beyond verifiability, there is a question of enforceability. Those who are skeptics of a cyber-warfare convention point, for example, to the provisions of the 1899 Hague Convention, which prohibited the bombardment of civilian targets.[118] Needless to say, the commitment to withhold bombing of civilian targets did not survive the World War II Blitz of London and the firebombing of Dresden (not to

113. *See, e.g.*, Kirk, *supra* note 89 (providing that many European countries are fearful that the Convention violates international law and state sovereignty and thus only thirty-nations have ratified its provisions).

114. THE WHITEHOUSE, *supra* note 111.

115. Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, *in* FUTURE CHALLENGES IN NATIONAL SECURITY AND LAW (Peter Berkowitz ed. 2011).

116. *Id.* at 4-5.

117. *Id.* at 10.

118. Geneva Convention Relative to the Protection of Civilian Persons in Time of War, art. 3 & 25, Aug. 12, 1949, 6 U.S.T. 3516.

mention the nuclear targeting of Hiroshima and Nagasaki).[119] There is, it is argued, therefore good reason to doubt that a prohibition on targeting electric grids (for example), would be sustainable in a truly significant conflict.[120] Notwithstanding these concerns, in 2009, the United States abandoned its position and agreed to discussions with Russia.[121]

As Jack Goldsmith of Harvard points out, in addition to the inherent inability to verify or enforce any cyber-disarmament treaty, the treaty would greatly limit America's freedom to act offensively in support of its own sovereign interests.[122] We would be bound to restrain the National Security Agency's operations in a host of ways to abide by the treaty's requirements. In addition, we would have to clean up our own house. In a 2010 survey by McAfee, the computer security company, more information-technology experts around the world expressed concern about the United States as a source of computer network attacks than about any other country.[123] And so we would likely be obliged to take steps to monitor the domestic Internet (and reign in our own hacker community) in compliance with our treaty obligations that would be a civil libertarian nightmare.

More significantly, the proposed treaty comes with some baggage. Non-Western states view the cyber domain less as a means of communication and more as a means of control – a viewpoint they want to import into any global treaty.[124] Consider the International Information Security agreement among the Shanghai Cooperation Organization ("SCO") nations (China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan).[125] Under the agreement state security and state control over information technologies and threats

119. *Nazi Germany Bombs London in First Day of the Blitz*, N.Y. TIMES (Sep. 7, 1940), http://learning.blogs.nytimes.com/2011/09/07/sept-7-1940-nazi-germany-bombs-london-in-first-day-of-the-blitz/. Conrad C. Crane, *Dresden: Air Attack On*, PBS (Feb. 13, 1949), http://www.pbs.org/thewar/detail_5229.htm.

120. Stewart Baker, *Denial of Service*, FOREIGN POL'Y (Sept. 30, 2011), http://www.foreignpolicy.com/articles/2011/09/30/denial_of_service?page=full.

121. John Markoff & Andrew E. Kramer, *In Shift, U.S. Talks to Russia on Internet Security*, N.Y. TIMES, Dec. 13, 2009, at A1.

122. Goldsmith, *supra* note 115.

123. STEWART BAKER, SHAUN WATERMAN, & GEORGE IVANOV, IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 30 (2010).

124. James Glanz & John Markoff, *U.S. Underwrites Internet Detour Around Censors*, N.Y. TIMES, June 12, 2011, at A1.

125. SHANGHAI COOPERATION ORG., http://www.sectsco.org/EN123/ (last visited Jan. 1, 2013).

are permitted.[126] In the view of the SCO nations the major threats to their own sovereignty are the "dominant position in the information space" of Western nations and the "dissemination of information harmful to the socio-political systems, spiritual, moral, and cultural environment of the States."[127]

### *G. Internet Freedom*

And that leads to another consideration America's interest in Internet freedom. We are often conflicted in that view, since freedom to use the Internet for political purposes often comes at the cost of decreased security on the network. But by and large we have come to see freedom of expression on the Internet as a fundamental "good." That is why Secretary of State Hillary Clinton emphasized that "[t]hose who disrupt the free flow of information in our society or any other pose a threat to our economy, our government, and our civil society."[128]

As a symbol of our view that freedom of expression is critical, the United States is leading efforts to develop the technology for a "shadow" Internet, one that can be deployed independent of the main backbone of the network.[129] If successful this new technology would, in effect, create an "Internet in a suitcase" and would enable dissidents to avoid the censorship of repressive authoritarian countries. To quote Secretary Clinton again, from an email correspondence with journalists James Glanz and John Markoff:

> We see more and more people around the globe using the Internet, mobile phones and other technologies to make their voices heard as they protest against injustice and seek to realize their aspirations. . . . There is a historic opportunity to effect positive change, change America supports. . . . So we're focused on helping them do that, on helping them talk to each other, to their communities, to their governments and to the world.[130]

In short, one aspect of the new multilateral policy calls for the development of norms that are squarely at odds with those espoused

126. Goldsmith, *supra* note 115, at 4.

127. *See* Tom Gjelten, *Seeing the Internet as an 'Information Weapon'*, NAT'L PUB. RADIO (Sept. 23, 2010, 12:00 AM), http://www.npr.org/templates/story/story.php?storyId=130052701 (providing background about the Shanghai Cooperation Organization's definition of cyberwar and its perspective on Western nations in the control of the Internet).

128. Hillary Clinton, Sec'y of State, Remarks on Internet Freedom (Jan. 21, 2010), *available at* http://www.state.gov/secretary/rm/2010/01/135519.html.

129. Glanz & Markoff, *supra* note 124.

130. *Id.*

by repressive governments. In that context, finding an international consensus is likely to prove very difficult.

### *H. The International Telecommunications Union*

So, if the Westphalian model leads to conflict and if the multilateral model involves disagreements that cannot be squared, why not go whole hog and create an international institution to run the Internet? Alas, that option, too, is problematic.

For years the architecture of the Internet has been defined by two NGO organizations, IETF and ICANN. Both are non-partisan and professional and their policy-making is highly influenced by nations that are technologically reliant on the Internet and have contributed the most to its development and growth.[131] As a consequence, America has an influential role in those organizations.

Many in the world see this as problematic. The International Telecommunications Union ("ITU") (which dates back to 1865, but is now a part of the United Nations[132]) has been proposed as a better model for Internet governance.[133] Transferring authority to the ITU (or a similar organization) is seen as a means of opening up the control of the Internet into a more conventional international process that dismantles what some see as the current position of global dominance of U.S. national interests.[134] In the ITU, like most U.N. institutions, a "one nation/one vote" rule applies–a prospect that would certainly diminish Western influence on Internet governance.[135]

Some argue that giving the ITU a role in Internet governance is no different from the role that the World Customs Organization has in setting shipping standards, or the International Civil Aviation Organization has in setting aviation traffic rules.[136] To some degree that may be true. On the other hand, aviation communications frequency requirements and standard shipping container sizes are not

131. Will Oremus, *Will the Internet Always be Run by Unelected Technocrats?*, SLATE (Jun. 20, 2012), http://www.slate.com/blogs/future_tense/2012/06/20/internet_governance_us_house_resolution_tells_un_to_butt_out.html.

132. INT'L TELECOMMUNICATION UNION, http://www.itu.int/en/history/overview/Pages/history.aspx (last visited Nov. 4, 2012).

133. Emma Llansó, *ITU: Internet Governance or Just Governing the Internet?*, CDT (Jun. 28, 2012), https://www.cdt.org/blogs/emma-llanso/2806itu-internet-governance-or-just-governing-internet.

134. Geoff Huston, *Opinion: ICANN, the ITU, WSIS, and Internet Governance*, 8 INTERNET PROTOCOL J. 1 (2005).

135. *Collection of the Basic Texts of the ITU Adopted by the Plenipotentiary Conference,* Chap. III INT'L TELECOMMUNICATION UNION Art. 32A, 117, http://www.itu.int/pub/S-CONF-PLEN-2011/en (2011).

136. JOVAN KURBALIJA & EDUARDO GELBSTEIN, ISSUES, ACTORS, AND DIVIDES 17 (Jovan Kurbalija & Eduardo Gelbstein eds. 2005).

fraught with political significance in the same way that the Internet has become. Rather those institutions succeed precisely because they manage the mundane, technical aspects of a highly specialized industry. They would be ill-suited to provide broadly applicable content regulation for a world-girding communications system. Thus, some fear that a transition to the ITU would run the risk of politicizing an already contentious domain even further.[137]

At bottom, however, the preference for ICANN over the ITU is not just about national interests. It is also, more fundamentally, about the contrast between ICANN's general adherence to a deregulated market-driven approach[138] and the turgid, ineffective process of the international public regulatory sector.[139] The American policy making apparatus is slow enough. The problem will, if anything, be exacerbated in the international sphere. Given the scale of the problem it is likely that the mechanisms for multinational cooperation are too cumbersome, hierarchical and slow to be of much use in the development of international standards. Acceptable behavior on the Internet mutates across multiple dimensions at a pace that far outstrips the speed of the policy-making apparatus within the U.S. government already – and the international system is immeasurably slower. Some are justifiably concerned that there is no surer way to kill the economic value of the Internet than to let the United Nations run it.[140]

Although there is a real intellectual appeal to the idea of an international governance system to manage an international entity like the Internet, the prognosis of a cybered Westphalian age is almost certainly the more realistic. We are likely to see the United States make common cause with trustworthy allies and friends around the globe to establish cooperative mechanisms that yield strong standards of conduct while forgoing engagement with multilateral organizations and authoritarian sovereigns.

## III. BILATERAL COOPERATION – THE UNITED STATES AND CANADA

The last topic for discussion is, in a narrow sense, a reiteration of our brief discussion of a FATF model for cybercrime. The most

137. *Id.* at 20.

138. Huston, *supra* note 134.

139. *Id.*

140. *See* Daniel Thomas, Richard Waters & James Fontanella-Khan, *The Internet: Command and Control*, FINANCIAL TIMES (Aug. 27, 2012), http://www.ft.com/cms/s/2/fab58818-e63a-11e1-ac5f00144feab49a.html#axzz2BHyRdsNE.

promising way forward, it seems, is for like-minded countries to cooperate as far as they can on common goals.

Canada and the United States have begun by recognizing that their intertwined economies necessarily mean an intertwined cyber domain.[141] As President Obama and Prime Minister Harper put it in their "Beyond the Border" declaration, the two countries are committed to "working together to prevent, respond to and recover from physical and cyber disruptions of critical infrastructure."[142] In doing that they will seek to work cooperatively "to strengthen the resilience of our critical and cyber infrastructure with strong cross-border engagement."[143] Both countries recognize that they benefit from their integrated infrastructures, but that they also share common vulnerabilities as evidenced by the statement, "Our countries intend to strengthen cybersecurity to protect vital government and critical digital infrastructure of national importance, and to make cyberspace safer for all our citizens."[144]

Given the intertwined nature of Canadian and American economic interests, this resolve to begin work on joint cybersecurity infrastructure protection efforts is welcome. Consider, as just one example, the massive interdependence of American and Canadian electric networks.[145] It does little good, say, for America to harden its electric generation infrastructure against a Stuxnet-like attack,[146] if a vulnerability in Ontario has catastrophic cross-border consequences. Likewise, Canadian protection of, say, the St. Lawrence Seaway, is of little value if America does not follow on. A joint approach to joint assets is both wise and essential.

With that perspective, the implementation of the Beyond the Border agreement is something of a disappointment. While the plan recognizes the critical importance of the cyber domain,[147] it is fair to

141. *See* AFP, *U.S., Canada Launch Joint Cybersecurity Plan*, SEC'Y WEEK (Oct. 26, 2012), http://www.securityweek.com/us-canada-launch-joint-cybersecurity-plan.

142. THE WHITEHOUSE, BEYOND THE BORDER: A SHARED VISION FOR PERIMETER SECURITY AND ECONOMIC COMPETITIVENESS (2011) [hereinafter BEYOND THE BORDER], *available at* http://www.Whitehouse.gov/the-press-office/2011/02/04/declaration-president-obama-and-prime-minister-harper-canada-beyond-bord

143. *Id.*

144. *Id.*

145. Joseph A. McKinney, *U.S.-Can. Energy Interdependencies*, 2 S. J. CAN. STUD. 1, 2 (2008) (discussing the economic forces and policy decisions that create interdependence between the U.S. and Can.).

146. Robert McMillan, *New Spy Rootkit Targets Industrial Secrets*, TECHWORLD (Jul. 19, 2010, 9:59 PM), http://news.techworld.com/security/3232365/new-spy-rootkit-targets-industrial-secrets/.

147. BEYOND THE BORDER, *supra* note 143, at iv.

say that most of the effort at this juncture is simply involved in defining the problem more that identifying joint solutions. Thus the Beyond the Border Action Plan[148] lists the following cyber-related tasks:

> Protect vital government and critical digital infrastructure of binational importance, and make cyberspace safer for all our citizens.
>
> Expand joint leadership on international cybersecurity efforts.[149]

While surely laudable goals they are rather modest in nature. For example, the way that the action plan says it will measure its success in protecting infrastructure is not, actually by attempting to determine if the infrastructure is actually better protected. Instead the plan says: "Measuring Progress: [Department of State] DOS, [Department of Homeland Security] DHS, and Public Safety Canada will report on joint or coordinated engagements with the private sector and external stakeholders, including joint briefings and presentations, assistance provided during the course of a cyber-incident, and joint communications products that are developed."[150] While engagement with the private sector is a means to the end, it is not, sadly, the end itself.

Likewise, in support of joint leadership in the international sphere, Canada promises to accede to the Cybercrime Convention;[151] the plan goes on to provide: "Measuring Progress: DOS and Public Safety Canada will report on the effectiveness of sharing cyber security best practices, the number of engagements with third countries, and how these efforts have translated into advancing American–Canadian objectives on cyber issues in international forums."[152] Again, good ideas but they will only get you so far.

To some degree the uncertainty of these goals is understandable. A fair reading of *Canada's Cybersecurity Strategy,*[153] suggests that, at this juncture, Canada has not done as much work as the United States in developing the domestic government infrastructure for operationalizing cybersecurity; the policies that will guide the use of those assets or the legal authorities that will permit effective action In

148. *Id.*

149. *Id.*

150. *Id.* at 23.

151. *Id.* at 24

152. *Id.* at 24.

153. GOV'T OF CAN., CANADA'S CYBER SECURITY STRATEGY: FOR A STRONGER AND MORE PROSPEROUS CANADA (2010), *available at* http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/_fl/ccss-scc-eng.pdf.

fact, Parliament is considering a bill to amend the Canadian criminal code to authorize greater government access to private internet communications in support of cybersecurity efforts.[154] Similar bills introduced in 2009 and 2010 failed to win the necessary approval.[155]

All of this is not, of course, to diminish Canada's effort, but simply to note that the scope of a coordinated response is, necessarily, limited by the existing capabilities of the two parties. The highest value of U.S.-Canadian cybersecurity cooperation is, at this juncture, probably American willingness to share best practices and other operational capacities. More saliently, in the end, the likely best of all possible worlds is for a joint services model of cybersecurity to be developed. Given the cyber threat to literally every sort of critical infrastructure and the inextricable nature of the U.S.-Canadian relationship, it seems to me that no other structure would be effective. When financial systems, electric grids, and air traffic controls are all, to some degree, shared, only a robust coordinated joint defense has any prospect of success.

154. *See, e.g.*, Protecting Children from Internet Predators Act, C-30, 41st Parliament (Can. 1st Sess. 2012).

155. *See, e.g.*, An Act to Amend the Criminal Code (Interception of Private Communications and Related Warrants and Orders), C-50, 40th Parliament (Can. 3rd Sess. 2010).