Penn State Law Review

Volume 119 | Issue 4 Article 6

3-1-2015

Brave New World: Challenges in International Cybersecurity Strategy and the Need for Centralized Governance

Susanna Bagdasarova

Brave New World: Challenges in International Cybersecurity Strategy and the Need for Centralized Governance

Susanna Bagdasarova*

ABSTRACT

In the past three decades, the Internet and related data system technologies have revolutionized nearly every aspect of daily life, making the word "cyberspace" a household term. Cyberspace, the field in which these technologies operate, is characterized by global reach and unlimited potential in terms of storage and communication. Billions of people worldwide use the Internet in their daily lives, and that number is only predicted to grow. Businesses, governments, and individuals increasingly depend on the Internet to store large amounts of information in these data systems. Unfortunately, as the use and types of uses of the Internet and data systems grow, so do potential security risks.

In the last few years, cybercrime has become a growing problem, affecting all types of Internet users and costing the world economy billions of dollars each year. Recognizing the global scope of these issues, the international community developed a series of conventions and strategies to respond to cyberthreats.

This Comment discusses the current state of international cybersecurity regulation by noting gaps and conflicts in the current regulatory regime. This Comment then discusses the most pressing concerns giving rise to the need for centralized regulation. Finally, this Comment recommends the creation of a global regulatory agency tasked with the development and enforcement of a coherent international cybersecurity regime.

* J.D. Candidate, The Dickinson School of Law of the Pennsylvania State University, 2015.

Table of Contents

I. INTRODUCTION

On April 27, 2007, the first strikes of what would become one of the worst cyberattacks in history hit the website of the Prime Minister of Estonia.[1] The attackers next disabled the websites of the president and government ministries, an act that paralyzed a self-described "paperless" government.[2] Within days, newspapers, television stations, schools, and banks experienced overwhelming traffic,[3] at one point causing Estonia's biggest bank to shut down its online service for over an hour.[4] Triggered by political anger over the relocation of a World War II monument, the

1. Steven Lee Myers, *Cyberattack on Estonia Stirs Fear of 'Virtual War'*, N.Y. TIMES, May 18, 2007, http://www.nytimes.com/2007/05/18/world/europe/18iht-estonia.4.5774234.html.

2. *Id.*

3. *Id.*

4. Mark Landler & John Markoff, *Digital Fears Emerge After Data Siege in Estonia*, N.Y. TIMES, May 29, 2007, http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0.

bulk of the assault involved denial-of-service attacks.[5] Hackers clogged Estonia's cyber-infrastructure in waves, infiltrating computers from around the world to magnify the level of network traffic.[6] The attacks increased network traffic by several thousand times the normal rate and crippled the small Baltic nation for over two weeks.[7]

Though not the first large-scale cybersecurity breach,[8] Estonia's experience, dubbed "Web War I,"[9] prompted a global conversation about cybersecurity.[10] The weaponization of cybertechnology not only revealed the vulnerabilities inherent in dependence on cyberspace but also brought the borderless nature of cyberspace into sharp relief.[11] Unlike a missile, traveling from one determinable geographic location to another through physical airspace, cyberattacks can travel internationally through cyberspace in moments, implicating computers in countries far from the original location of the hacker.[12] During Web War I, for example, hackers remotely rerouted attacks through unsuspecting computers in other countries such as the United States and Vietnam, thus prolonging and complicating efforts to respond and investigate.[13]

Other countries have experienced similar cyberattacks.[14] In 2010, a sophisticated cyberweapon named Stuxnet[15] infected industrial sites and

---

5. *See id.*; *infra* note 49 (explaining denial-of-service attacks).

6. *See* Landler & Markoff, *supra* note 4.

7. *See id.*

8. *See* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 829 (2012) (describing "Titan Rain," a U.S. cybersecurity breach in 2003 which leaked sensitive information to Chinese hackers).

9. *War in the Fifth Domain*, ECONOMIST, July 1, 2010, http://www.economist.com/node/16478792.

10. *See* Landler & Markoff, *supra* note 4 (discussing the possibility of NATO reexamining its commitment to collective defense in light of emerging cyberthreats).

11. *See id.* (discussing the technical methods by which hackers flooded Estonia's servers, including infecting computers around the world with software to create "zombies" that would then send traffic to Estonian websites).

12. *See id.*

13. *See id.*

14. *See id.* (noting cyberattacks in the Middle East and Eastern Europe).

15. Stuxnet is a software "worm" that infects computers running on Microsoft Windows software. *See How Stuxnet Works: What the Forensic Evidence Reveals*, TELEGRAPH (Jan. 21, 2011), http://www.telegraph.co.uk/technology/8274488/How-Stuxnet-works-what-the-forensic-evidence-reveals.html. Introduced into the Iranian computer system via an infected memory stick plugged into a computer's USB port, the worm ordered the centrifuges at the facility to spin at extremely high speeds for short periods. *See id.* To delay detection of the damage, Stuxnet recorded normal operations at the plant and played back the readings to plant operators during the attacks. *See* William J. Broad, John Markoff & David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES, Jan. 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all&r=0.

nuclear facilities across Iran.[16] The attacks devastated the nation's nuclear program, destroying nearly 1000 of the country's 6000 nuclear centrifuges and severely damaging the Natanz Enrichment Complex, Iran's primary uranium enrichment facility.[17] Later confirmed to be a joint cyberattack on the Iranian nuclear program by the United States and Israel, the incident provided a glimpse into the future of cyberwarfare, with attacks in the cyber-realm compromising assets in the physical realm.[18]

Governments are not the only entities affected by breaches in cybersecurity.[19] In recent years, major companies such as Sony, Visa, and Mastercard have experienced cyberattacks that exposed confidential information and required significant system repair.[20] In the 21st century, many aspects of life involve the Internet, making nearly any entity or individual using the Internet vulnerable to a cyberattack.[21] Functioning information networks provide the backbone of governments, financial institutions, businesses, electricity and water infrastructures, and the military.[22] Individuals rely heavily on cybertechnology for work, banking, shopping, communication, and entertainment.[23]

As dependence on cybertechnology increases in nearly every sector of the government and economy, cybercrime increases as well.[24] Each

16. Broad, Markoff & Sanger, *supra* note 15.

17. *See id.*; *Natanz Enrichment Complex*, NUCLEAR THREAT INITIATIVE (Sept. 24, 2013), http://www.nti.org/facilities/170/; *see also* Ellen Nakashima & Joby Warrick, *Stuxnet Was Work of U.S. and Israeli Experts, Officials Say*, WASH. POST (June 2, 2012), http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

18. Nakashima & Warrick, *supra* note 17 (quoting one cyber-expert: "'This officially signals the beginning of the cyber arms race in practice and not in theory'").

19. Brian B. Kelly, Note, *Investing in a Centralized Cybersecurity Infrastructure: Why "Hacktivism" Can and Should Influence Cybersecurity Reform*, 92 B.U.L. REV. 1663, 1664–68, 1680 (2012) (discussing cybersecurity breaches involving various entities, including Sony, PayPal, and San Francisco's Bay Area Rapid Transit system).

20. *See id.* at 1664–65, 1680.

21. *See Joint Communication to the European Parliament, the Council of European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, at 2–3, COM (2013) 1 final (July 2, 2013) [hereinafter *Cybersecurity Strategy of the European Union*].

22. *See* EXEC. OFFICE OF THE PRESIDENT, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY SECURITY, AND OPENNESS IN A NETWORKED WORLD 2 (2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (describing various uses for cybertechnology).

23. *See id.* at 3. Cyberspace has even become a medium for the growth of social and political movements, prompting Egypt to shut down access to the Internet during its 2011 revolution. James Glanz & John Markoff, *Egypt Leaders Found 'Off' Switch for Internet*, N.Y. TIMES, Feb. 15, 2011, http://www.nytimes.com/2011/02/16/technology/16internet.html?pagewanted=all.

24. *See Cybersecurity Strategy of the European Union*, *supra* note 21, at 2–3.

use of cybertechnology exposes the user to potential cybersecurity threats.[25] While many of these threats are handled without incident,[26] damaging incidents, such as Estonia's 2007 attack, are not uncommon.[27]

Unsurprisingly, cybersecurity has become a significant area of international and domestic concern.[28] Increasing dependence on cybertechnology has prompted many countries to develop strategies to regulate actions in cyberspace and improve cybersecurity.[29] Accordingly, the United States and the European Union released cybersecurity strategies in 2011 and 2013, respectively.[30] Both the United States strategy ("U.S. Strategy") and the European Union strategy ("EU Strategy") address the growing significance of cybertechnology in daily life and the need to create viable regulations.[31]

The greater field of international cyberspace regulation currently consists of a wide variety of national strategies, conventions, summits, agreements, and organizations.[32] Although some overlap and collaboration exists, the piecemeal nature of the current international cybersecurity regime leaves open gaps in policy and security.[33] To fill these gaps, it is necessary to approach an international cybersecurity regime not as geographically divided parts, but as a unified whole in a borderless cyberspace.[34] The international community should develop a global regulatory body for cyberspace and, in doing so, should look to other examples of centralized international regulation.[35]

---

25. *See id.*

26. For example, the Pentagon reports ten million cyberattack attempts a day. Zachary Fryer-Biggs, *U.S. Military Goes on Cyber Offensive*, DEFENSE NEWS (Mar. 24, 2012), http://www.defensenews.com/article/20120324/DEFREG02/303240001/U-S-Military-Goes-Cyber-Offensive.

27. *See* Hathaway et al., *supra* note 8, at 819, 829 (describing various cyberattacks against countries including the United States and Burma).

28. *Cybersecurity Strategy of the European Union*, *supra* note 21, at 3 (noting that "governments across the world have started to develop cybersecurity strategies and to consider cyberspace as an increasingly important international issue").

29. *See id.*

30. *See generally* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22; *Cybersecurity Strategy of the European Union*, *supra* note 21, at 1.

31. EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 3-4; *Cybersecurity Strategy of the European Union*, *supra* note 21, at 3.

32. *See* William M. Stahl, Note, *The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity*, 40 GA. J. INT'L & COMP. L. 247, 263–65 (2011) (outlining existing international cybersecurity regulations); *see also infra* Part II.D (discussing the current international cybersecurity regime and noting significant treaties and organizations).

33. *See Cybersecurity Strategy of the European Union*, *supra* note 21, at 9 (noting gaps in national cybersecurity capabilities of member states).

34. *See infra* Part II.C.1 (discussing borderlessness as an inherent characteristic of cyberspace).

35. *See infra* Part IV.

This Comment will provide an in-depth examination of the current field of international cyberspace regulation to illustrate the need for centralized regulation. Part II will introduce the concepts of cyberspace, cybercrime, and cybersecurity and contextualize them within the current international cybersecurity regime. Part III will discuss the most pressing concerns giving rise to the need for centralized regulation and analyze how the cybersecurity strategies of the United States and the European Union seek to answer these concerns. Part IV will offer a recommendation to create a global regulatory agency to meet the specific needs of cyberspace and cybersecurity regulation. Finally, Part V will offer a brief conclusion.

II. DEFINING CONCEPTS AND DEVELOPING CONTEXT

To understand the growing need for centralized cybersecurity regulation, it is critical to define key cyber-concepts and outline the existing regulatory regime. The three central concepts are: (1) cyberspace, the realm in which information is exchanged and stored;[36] (2) cybercrime, various harmful and illegal activities occurring within that realm;[37] and (3) cybersecurity, a system of tools, policies, and practices aimed at protecting information and assets in cyberspace.[38] Additionally, cyberspace is defined by unique characteristics that pose regulatory difficulties, and the current regulatory regime is composed of a patchwork of national and international strategies and organizations.[39] This Part will summarize these main concepts and the current regime in order to better contextualize the discussion.

A. Cyberspace

Despite its ubiquity, "cyberspace" has proven difficult to define, both as a result of its relative novelty and because of the permeable and protean nature of its borders.[40] As one court explained simply and functionally, cyberspace is a "world of electronic communications over computer networks."[41] Scholars, on the other hand, have defined cyberspace in more complex terms. One scholar defined cyberspace as

36. *See infra* Part II.A.
37. *See infra* Part II.B.
38. *See infra* Part II.B.
39. *See infra* Part II.C–D.
40. *See* Lance Strate, *The Varieties of Cyberspace: Problems in Definition and Delineation*, 63 W. J. OF COMM. 382, 382–83 (1999) (examining various issues in defining cyberspace and creating a detailed taxonomy to aid in its discussion and understanding).
41. Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc, 907 F. Supp. 1361, 1365 n.1 (N.D. Cal. 1995).

an "evolving man-made domain for the organization and transfer of data . . . a combination of private and public property governed by technical rule sets designed primarily to facilitate the flow of information."[42]

Novelist William Gibson, whose book *Neuromancer* contains one of the first references to the word "cyberspace,"[43] offered an early, colorful definition of the term as "[a] consensual hallucination experienced daily by billions of legitimate operators . . . . A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data."[44] Though not couched in legal or academic terms, Gibson's definition perhaps best conveys the complexity, vastness, and unlimited potential of cyberspace—characteristics to keep in mind when analyzing issues of vulnerability and regulation.

B. Cybercrime and Cybersecurity

The greater the volume of valuable data that individuals and entities store and exchange in cyberspace, the more such information is at risk.[45] This phenomenon increases the need for improved security.[46] Many security risks fall under the umbrella of cybercrime, which refers to criminal activities in which a computer or information system is either the primary tool or target of attack[47] and includes a wide variety of offenses, such as fraud, identity theft, incitement to racial violence,[48] denial-of-service,[49] and malware.[50]

Correspondingly, the field of cybersecurity encompasses a wide range of protections, which can vary depending on the identity of the user being protected.[51] For individuals, the focus of cybersecurity is

---

42. Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F. L. REV. 65, 68 (2009).

43. *See* Strate, *supra* note 40, at 7.

44. WILLIAM GIBSON, NEUROMANCER 51 (1984).

45. *See Cybersecurity Strategy of the European Union, supra* note 21, at 3.

46. *See id.*

47. *See id.*

48. *See id.* at 3 n.5.

49. Denial-of-service attacks occur when a large number of computers are used to simultaneously request information from a single website, overwhelming the server and rendering the site inaccessible. United States v. Raisley, 466 F. App'x 125, 127 (3d Cir. 2012).

50. *Cybersecurity Strategy of the European Union, supra* note 21, at 3 n.5. Malware (malicious software) is a type of software that can cause damage to computer performance and compromise its security. Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1171 (9th Cir. 2009).

51. *See Cybersecurity Strategy of the European Union, supra* note 21, at 18.

typically protection against identity or data theft,[52] whereas for businesses, the focus is usually prevention of fraud or forgery.[53] On a broader scale, when the user is an entire nation or government, cybersecurity addresses protection from cyberterrorist attacks[54] or possible cyberwarfare.[55]

C. *Challenges to Effective Cyberregulation*

In light of emerging cybersecurity threats, many governments have recognized the need to formally address these issues, both nationally and internationally.[56] However, four characteristics of cyberspace, and their interactions with one another, pose challenges to the development of effective cybersecurity regimes.[57] Cyberspace is: (1) global and decentralized,[58] (2) anonymous,[59] (3) pervasive,[60] and (4) constantly and rapidly evolving.[61] By using these challenges as guideposts, the international community may be able to successfully regulate cyberspace on a global level.

1. Global and Decentralized

Perhaps the most significant and unique characteristic of the Internet is its function as an inherently borderless medium of communication.[62] The Internet is not a physical place but a "network of networks" that allows individuals with access to network-connected computers to exchange information nearly instantaneously, regardless of

52. *See id.* at 3.
53. *See id.*
54. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 20 (outlining U.S. policy in combating cybercrime internationally through collaboration and the rule of law).
55. *See id.* at 4 (recognizing the potential for traditional forms of international conflict to extend into cyberspace).
56. *See Cybersecurity Strategy of the European Union*, *supra* note 21, at 3.
57. *See infra* Part II.C (discussing the four challenging characteristics of cyberspace in detail).
58. *See infra* Part II.C.1.
59. *See infra* Part II.C.2.
60. *See infra* Part II.C.3.
61. *See infra* Part II.C.4.
62. *See* Jessica E. Bauml, *It's a Mad, Mad Internet: Globalization and the Challenges Presented by Internet Censorship*, 63 FED. COMM. L.J. 697, 703 (2011) (noting that the lack of borders gave rise, in the 1990s, to "a general concern that the challenges the Internet presented to governing bodies would ultimately diminish the relevance of the nation-state all together").

where the individual is physically located.[63] This system of networks is not only borderless within a nation, but also internationally.[64]

This limitless reach does create problems in terms of cybersecurity.[65] The decentralized nature of the Internet is evident in the lack of an institutional owner or administrator of the underlying technical infrastructure,[66] command center, or single storage location for information.[67] Cross-border threats have emerged as a result of this constant and simultaneous interaction between various users.[68] Combating these threats requires consideration of additional issues of enforcement, jurisdiction, and conflicts of law,[69] as there is no entity, institution, or single physical location to be regulated.[70]

2. Anonymous

Another characteristic of cyberspace that poses a challenge to effective regulation is the anonymity it provides to its users.[71] As noted by Justice O'Connor in her dissent in *Reno v. ACLU*,[72] cyberspace is fundamentally different from the physical world in that its nature as a system of interconnected data pathways allows users to easily mask their identities.[73] Although courts have noted that anonymity has proven to be a positive force in the development of the Internet as a marketplace for ideas,[74] anonymity also poses a challenge to cybersecurity policy.[75] The

63. *See* ACLU v. Reno, 929 F. Supp. 824, 830–32 (E.D. Pa. 1996) (outlining an in depth history of the Internet and its use in the United States as well as discussing First Amendment free speech protections as they apply to the Internet).

64. *See id.*

65. *See Cybersecurity Strategy of the European Union*, *supra* note 21, at 3.

66. *See* ACLU v. Reno, 929 F. Supp. at 832.

67. *Id.*

68. *See Cybersecurity Strategy of the European Union*, *supra* note 21, at 3.

69. *See* Council of Europe Convention on Cybercrime ch. II, Nov. 23, 2001, T.I.A.S. No. 13,174, ETS No. 185 (calling for a harmonization of international cybercrime law and laying out procedures for investigation and prosecution). The Convention on Cybercrime is one of the most significant components of the current international cybersecurity regime. *See infra* Part II.D.2.

70. *See* ACLU v. Reno, 929 F. Supp. at 832.

71. Reno v. ACLU, 521 U.S. 844 (1997) (O'Connor, J., dissenting) (discussing the implications of anonymity for law enforcement regulation).

72. Reno v. ACLU, 521 U.S. 844 (1997) (holding certain provisions of the Communications Decency Act unconstitutional in that they abridged First Amendment free speech on the Internet).

73. *Id.* at 889–90 (O'Connor, J., dissenting).

74. *See e.g.*, Doe v. 2themart.com Inc., 140 F. Supp. 2d 1088, 1093 (W.D. Wash. 2001) ("Internet anonymity facilitates the rich, diverse, and far ranging exchange of ideas."); Quixtar Inc. v. Signature Mgmt. Team, LLC, 566 F. Supp. 2d 1205, 1213–14 (D. Nev. 2008) (noting that the court must balance First Amendment free speech protections of anonymity with the interests of the discovery-seeking party when ruling on a motion to compel discovery of the identities of anonymous Internet users).

relative ease with which one can conceal one's identity aids cybercriminals in carrying out attacks on computers and data systems.[76] Additionally, anonymity may cause difficulties in investigating crimes when they occur.[77]

3. Pervasive

A third challenging characteristic of cyberspace is its growing pervasiveness in the last two decades.[78] Since the commercialization of the Internet in the early 1990s,[79] Internet users have grown to comprise nearly 40 percent of the world's population and 77 percent of the population of the developed world.[80] In the first decade of the 21st century, Internet use rose dramatically, with five times more users in 2010 than in 2000.[81] Part of the reason the Internet is so pervasive is its widespread availability.[82] Furthermore, computer and Internet technologies have become indispensible to daily life, with businesses, governments, and individuals depending more on electronic data systems for a variety of needs.[83]

4. Constantly and Rapidly Growing

Finally, not only is the Internet pervasive, but its use and reach is growing exponentially.[84] As cyberspace expands, so does dependence on the technologies that make up cyberspace.[85] Together, pervasiveness and

75. *See Cybersecurity Strategy of the European Union*, *supra* note 21, at 9.

76. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 4.

77. *See id.* (noting that "the ability to establish an anonymous virtual presence can also lead to 'safe havens' for criminals, with or without a state's knowledge").

78. Rajiv C. Shah & Jay P. Kesan, *Privatization of the Internet's Backbone Network*, 51 J. BROADCASTING & ELECTRONIC MEDIA 93, 98–100 (2007).

79. *Id.*

80. Press Release, Int'l Telecomm. Union, ITU Releases Latest Global Technology Development Figures (Feb. 27, 2013) (announcing findings that by the end of 2013, 2.7 billion people, or 39% of the world's population, will be using the Internet).

81. *The Incredible Growth of the Internet Since 2000*, ROYAL PINGDOM (Oct. 22, 2010), http://royal.pingdom.com /2010/10/22/incredible-growth-of-the-internet-since-2000 (compiling statistics on Internet growth between 2000 and 2010 and noting that within that time frame, Internet users jumped from 361 million to almost two billion).

82. *See* ACLU v. Reno, 929 F. Supp. 824, 832–34 (E.D. Pa. 1996) (noting that individuals may access the Internet through educational institutions, libraries, workplaces, and at-home paid subscriptions to an Internet service provider).

83. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 3 (describing various industries and areas which increasingly depend on digital infrastructure, including electricity and water, government, financial systems, and social and political movements).

84. *See* Firth v. State, 775 N.E.2d 463, 465 (N.Y. 2002).

85. United States v. Voelker, 489 F.3d 139, 148 n.8 (3d Cir. 2007) (holding that a ban on any computer equipment or on-line computer service as a condition of a lifetime

growth result in a simultaneous deepening and broadening of individual and institutional reliance on cybertechnology.[86] In turn, security vulnerabilities grow and are exacerbated by the speed of technological development and the ease of achieving anonymity online.[87] As the use and types of uses of the Internet expand, traditional crimes and conflicts will extend into cyberspace.[88] Lawmakers must keep up with the extension of crime into cyberspace and create appropriate responses.[89]

The nebulous nature of cyberspace, however, along with user anonymity and the irrelevance of physical distance, are challenges not present in proscribing crime in the physical world.[90] Thus, regulation of cybercrime is not merely the application of existing law to cyberspace.[91] Governments must consider the challenging interaction of the above-described characteristics within the decentralized and borderless context of cyberspace in order to develop effective strategies for regulation.

D. Cyberregulation in Context

In the last several years, many countries have developed individual cybersecurity strategies.[92] The last decade has also seen the rise of international cooperation in the form of summits, regulations, conventions, and treaties seeking to create standards and norms in cyberspace.[93] Briefly analyzing key conventions and organizations reveals both the gaps in current regulation and uncovers tools for building a global regulatory regime.

1. International Telecommunication Union

One of the most significant building blocks of the current international cybersecurity regime is the International

---

term of supervised release to be overly broad and unworkable, particularly in light of the level of incorporation such technology has in day-to-day life).

86. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 3 (discussing the increasing uses of cybertechnology as well as the growth of Internet use in the last half century).

87. *See Cybersecurity Strategy of the European Union*, *supra* note 21, at 2-3, 9.

88. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 4.

89. *See* Reno v. ACLU, 521 U.S. 844, 888–92 (1997) (O'Connor, J., dissenting) (discussing the difficulties of creating "adult zones" in cyberspace and noting developing technology created to enhance law enforcement in cyberspace).

90. *See id.* at 889–91 (discussing geography and identity as markers that enable the enforcement of criminal law in the physical world but that do not have exact analogues in cyberspace). Justice O'Connor noted that traditional methods of regulation must be reevaluated and modified in light of these differences. *Id.*

91. *See id.*

92. *See Cybersecurity Strategy of the European Union*, *supra* note 21, at 3.

93. *See* Stahl, *supra* note 32, at 263–65.

Telecommunication Union ("ITU").[94] A specialized agency of the United Nations ("UN"),[95] the ITU is an intergovernmental organization that focuses on key issues concerning information and communication technologies, including coordination, access, and development.[96] In recent years, the ITU has recognized increasing cross-border threats to cybersecurity and has noted the need to improve international cooperation in the development of appropriate protective and punitive mechanisms.[97] One of the ITU's most pertinent initiatives is the Global Cybersecurity Agenda (the "Global Agenda"), the goal of which is "to provide a framework within which an international response to the growing challenges to cybersecurity can be coordinated and addressed."[98]

The Global Agenda recognizes that the absence of an overarching organizational structure, coupled with legal loopholes within and between nations, leaves individuals and nations vulnerable to cyber threats.[99] Suggested actions include harmonizing cybercrime legislation, standardizing technical security measures, and creating organizational structures for further cyberregulation development.[100] Despite the Global Agenda's collaborative vision for standardizing international

94. Constitution and Convention of the International Telecommunication Union, *reprinted in* FINAL ACTS OF THE PLENIPOTENTIARY CONFERENCE 24 (1992) [hereinafter ITU Constitution and Convention].

95. *See id.*

96. *See id.* at 3–5; *infra* notes 209–10, 218 and accompanying text(discussing the possibility of ITU cooperation with a global cyberregulatory agency).

97. ITU, *Strengthening the Role of ITU in Building Confidence and Security in the Use of Information and Communication Technologies*, ITU Admin Council Res. No. 130 (2010), *reprinted in* COLLECTION OF THE BASIC TEXTS OF THE INTERNATIONAL TELECOMMUNICATION UNION ADOPTED BY THE PLENIPOTENTIARY CONFERENCE 450–52 (2011).

98. *Global Cybersecurity Agenda*, INT'L TELECOMM. UNION 12, http://www.itu.int/osg/csd/cybersecurity/gca/new-gca-brochure.pdf (last visited Feb. 4, 2014); *see infra* Part IV.B (discussing the Global Agenda in the context of a global cyberregulatory agency).

99. *Global Cybersecurity Agenda*, *supra* note 98, at 10. In 2008, the International Multilateral Partnership Against Cyber Threats ("IMPACT") became the operational home of the Global Agenda. *International Multilateral Partnership Against Cyber* Threats, INTERNATIONAL TELECOMMUNICATION UNION 4-5(2011), *http://www.itu.int/ITU-D/cyb/publications/2012/IMPACT/IMPACT-en.pdf.* IMPACT is a global public-private alliance against cyberthreats whose mission is to bring various stakeholders, including governments, industry, and academics, to develop policies and resources to enhance global capability for dealing with cyber threats. *See id.* As of 2011, IMPACT is the ITU's cybersecurity executing arm, responsible for providing cybersecurity assistance and support to the ITU's member states, including the United States and EU nations, and UN organizations. *See id*; *see also infra* notes 209–10 and accompanying text (discussing IMPACT's potential role in supporting a global cyberregulatory agency).

100. *Global Cybersecurity Agenda*, *supra* note 98, at 14–20, 28–29.

cybersecurity regulations, it is a suggested framework, not a binding treaty.[101]

2. Convention on Cybercrime

Another international agreement that has influenced the current state of cybersecurity is the Convention on Cybercrime.[102] Also known as the Budapest Convention, the Convention on Cybercrime is a 2001 international treaty drafted by the Council of Europe[103] to address the growing problem of cybercrime.[104] The Convention on Cybercrime aims to harmonize domestic laws in order to streamline criminal investigations and prosecutions of crimes involving computer systems and data.[105]

Key cybersecurity violations addressed by the Convention on Cybercrime include forgery, fraud, copyright infringement, and child pornography.[106] Signatories to the Convention on Cybercrime are tasked with adopting legislative measures to establish procedures as outlined in the treaty,[107] as well as cooperating with one another through mutual assistance in the absence of pertinent agreements.[108] The United States, a non-member of the Council of Europe, and every European Union member state has signed the treaty, thus indicating their recognition of and support for a more cooperative cybersecurity regime.[109]

3. Additional Protocol to the Convention on Cybercrime

As a supplement to the Convention on Cybercrime, the Council of Europe developed the Additional Protocol to the Convention on

101. *See id.* at 8.

102. *See* Council of Europe Convention on Cybercrime, Nov. 23, 2001, T.I.A.S. No. 13,174, ETS No. 185; *see also infra* Part IV.B (discussing the Convention on Cybercrime as a possible template for a global cyberregulatory agency's regulations).

103. The Council of Europe is an international organization whose aim is to promote cooperation between European nations in order to facilitate economic and social progress and who focuses on fostering unity through the development of legal standards, common actions, and the realization of human rights. *See* Statute of the Council of Europe, art. 1, May 5, 1949, 87 U.N.T.S. 103.

104. *See* Council of Europe Convention on Cybercrime, *supra* note 102, at pmbl.

105. *See id.*

106. *See id.* at ch. II § 1 tit. 2.

107. *See id.* at ch. II § 2 tit. 1 art. 14.

108. *See id.* at ch. III.

109. *See* Council of Eur., *Convention on Cybercrime*, http://conventions.coe.int/Treaty/Commun/print/ChercheSig.asp?NT=185&CL=ENG (last updated Feb. 1, 2014) (listing the signatories of the Convention on Cybercrime and indicating that the treaty has been ratified by the United States and 36 members of the Council of Europe).

Cybercrime (the "Protocol") in 2006.[110] The Protocol is a response to "acts of a racist and xenophobic nature [that] constitute a violation of human rights and a threat to the rule of law and democratic stability."[111] Nations that have adopted the Protocol are required to criminalize the dissemination of xenophobic acts through computer systems.[112] Unlike the Convention on Cybercrime, the Protocol lacks support from the United States and several European Union member states,[113] underscoring the lack of standardized international regulation in cyberspace and gaps in existing enforcement.

4. European Cybercrime Center

A recent but promising development in the field of international cybersecurity is the European Cybercrime Centre (the "Cybercrime Centre").[114] Formed in January 2013, the Cybercrime Centre is a European Union organization established to coordinate cross-border law enforcement against cybercrime.[115] The Cybercrime Centre intends to fulfill a variety of initiatives, including raising awareness, developing best practice on cybercrime investigations, and providing training to combat cybercrime.[116] Perhaps the most significant aspect of the Cybercrime Centre is its function as the European information hub on cybercrime.[117] This function will centralize at least some information on cybercrime, likely enabling the Cybercrime Centre to more successfully launch targeted investigations and protective measures.[118]

III. COMPARISON OF THE STRATEGIES

The foregoing discussion is not a comprehensive view of cyberspace and the international cybersecurity regime.[119] However, the uniquely challenging characteristics of cyberspace and the differing

110. Additional Protocol to the Convention on Cybercrime, Jan. 28, 2006, ETS No. 189.

111. *Id.* at pmbl.

112. *Id.* at art. 3.

113. Council of Eur., *Additional Protocol to the Convention*, http://conventions.coe.int/treaty/Commun/ChercheSig.asp?NT=189&CM=&DF=&CL=ENG (last updated Feb. 1, 2014).

114. *See* Bruce Zagaris, *EU Opens European Cybercrime Center (EC3) at Europol*, 29 INT'L ENFORCEMENT L. REP. 111, 111 (2013); *see also infra* Part IV.C (noting that the Cybercrime Centre could serve as a model for a global cyberregulatory agency).

115. *See* Zagaris, *supra* note 114, at 111.

116. *Id.*

117. *See id.*

118. *See id.*

119. For an in-depth overview of existing international law on cybercrime, see Stahl, *supra* note 32, at 263-65.

points of origin, missions, and methodologies of the current regulatory organizations reveal a borderless domain of interaction without a unified approach to regulation, despite the significant potential dangers of cybersecurity breaches.[120] Centralized international regulation will provide an effective remedy for these concerns. This Part will analyze the three main concerns giving rise to the need for centralized regulation: national security, economic prosperity, and government transparency. This Part will also analyze the ways in which two major national/regional cybersecurity strategies, the U.S. and EU strategies,[121] attempt to resolve these issues and why such an individual method of regulation will not succeed in cyberspace.

A. National Security

The first major concern giving rise to the need for centralized regulation is national security. Financial institutions, militaries, and governments have become increasingly dependent on cybernetworks.[122] As a result, cyberattacks, whether by criminals or states, can lead to devastating results.[123] For example, undetectable until after the damage had been done, the Stuxnet worm, jointly created by the United States and Israel, surreptitiously and severely damaged Iran's nuclear program

120. *See supra* Part II.

121. In the last four years, both the United States and the European Union have developed strategies to address the growing need for cybersecurity regulation both domestically and internationally. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 1–2; *Cybersecurity Strategy of the European Union*, *supra* note 21, at 1–3. Together, the strategies of the United States and the European Union represent 29 Western countries. *Member Countries of the European Union*, EUROPEAN UNION, http://europa.eu/about-eu/countries/member-countries/index_en.htm (describing the European Union's 28 countries). Furthermore, combined, the United States and the European Union comprise approximately one quarter of the world's Internet usage. *See Internet Usage in the European Union*, INTERNET WORLD STATISTICS (June 30, 2012), http://www.internetworldstats.com/stats4.htm (finding that, as of 2012, the European Union comprises 15.3% of the world's Internet users); *Internet Usage Statistics for All the Americas*, INTERNET WORLD STATISTICS (June 30, 2012), http://www.internetworldstats.com/stats2.htm (finding that, as of 2012, the United States has approximately a quarter-billion, or 10.2%, of the world's Internet users). Therefore, although a number of other nations have developed cybersecurity policies, the strategies of the United States and the European Union are particularly helpful in providing insight into the future of international cybersecurity in developed Western nations. *See Cybersecurity Strategy of the European Union*, *supra* note 21, at 3 (noting cybersecurity strategies from the United Kingdom, France, and Russia).

122. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 3.

123. *See* Landler & Markoff, *supra* note 4 (describing the effects of large-scale cyberattacks on Estonia).

without engaging any traditional weapons.[124] The attack was later labeled an "act of force" by a research team from the North Atlantic Treaty Organization (NATO),[125] which noted that the attack was also likely illegal under international law.[126] Although Stuxnet attacked a uranium-enrichment facility not directly connected to civilian life, it is not hard to imagine a scenario in which a cyberattack targets critical domestic infrastructure, such as the water supply.[127]

More recently, China has revealed the existence of specialized cyberwar-capable units in its military and intelligence operations.[128] In addition, "some five dozen countries are building a military-cyber operation."[129] As technology continues to advance, nations may view cybertechnology as a more and more viable means of espionage and warfare.[130] To combat a potential "MAD"[131] scenario in 21st century cyberspace, uniform, global regulation is needed. Perhaps even more worrying is the potential for cyberterrorism and the difficulty of prevention and investigation in cyberspace.[132]

The U.S. and EU Strategies diverge on the issue of national defense in cyberspace.[133] Improving military cyberdefense capabilities is a separate and unique policy priority in the U.S. Strategy,[134] both internally

124. Nakashima & Warrick, *supra* note 17 ("Effectively the United States has gone to war with Iran and has chosen to do so in this manner because the effects can justify this means.").

125. NATO is a military and political alliance comprised of 28 countries. *What is Nato?*, U.S. DEP'T OF STATE, http://www.state.gov/p/eur/rt/nato/nato2012/about/ (last visited Mar. 28, 2015).

126. Shaun Waterman, *U.S.-Israeli Cyberattack on Iran Was 'Act of Force,' NATO Study Found*, WASH. TIMES (Mar. 24, 2013), http://www.washingtontimes.com/news/2013/mar/24/us-israeli-cyberattack-on-iran-was-act-of-force-na/?page=all.

127. *See generally* Srinivas Panguluri et al., *Protecting Water and Wastewater Infrastructure from Cyber Attacks*, 5 FRONTIERS EARTH SCI. 406 (2011).

128. Shane Harris, *China Reveals Its Cyberwar Secrets*, DAILY BEAST (Mar. 18, 2015), http://www.thedailybeast.com/articles/2015/03/18/china-reveals-its-cyber-war-secrets.html.

129. *Id.*

130. *See* Dan Holden, *Is Cyber-Terrorism the New Normal?*, WIRED, http://www.wired.com/2015/01/is-cyber-terrorism-the-new-normal/ (last visited Mar. 19, 2015).

131. MAD, or mutually assured destruction, describes a doctrine wherein two countries each have a large enough nuclear store to destroy the other side and, should one country be attacked, the other would retaliate in kind. *See generally* GETTING MAD: NUCLEAR MUTUAL ASSURED DESTRUCTION, ITS ORIGINS AND PRACTICE (Henry D. Sokolski ed. 2004).

132. *See* Holden, *supra* note 130.

133. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 20–21; *Cybersecurity Strategy of the European Union*, *supra* note 21, at 11–14.

134. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 20–21.

and externally.[135] Internally, the U.S. Strategy notes the need to protect the military's increasing dependence on cybertechnology.[136] Externally, the strategy discusses the need to develop military alliances in order to enhance collective self-defense in cyberspace.[137]

Conversely, the EU Strategy does not address national security concerns in the same way.[138] The military is chiefly mentioned in the context of coordination with civilian actors to develop cybersecurity best practices.[139] The EU Strategy does recommend harmonized legislation as the first step in reducing cybercrime and increasing cyber resilience.[140] The proposals suggest creating minimum cybersecurity requirements for all European Union member states[141] and urge ratification and implementation of the Convention on Cybercrime by non-signatories.[142]

Despite the recognition by both strategies that regulation necessitates international and multi-stakeholder collaboration,[143] the potentially debilitating dangers of cyberwar and cyberterrorism militate in favor of more uniform regulation and enforcement. The lack of a harmonized approach by these two major strategies indicates the likelihood of a disjointed international approach to a major international security threat, a dangerous possibility in the face of rising cyberterrorism.[144] A centralized response system will be better equipped to develop and control the weaponization of cybertechnology, and such centralization is not unprecedented.[145]

B. Economic Prosperity

A second major concern giving rise to the need for centralized regulation is economic prosperity and security. Between 2006 and 2011, the Internet "accounted for 21 percent of the GDP growth in mature

135. *See id.*
136. *See id.* at 20.
137. *See id.* at 21.
138. *See Cybersecurity Strategy of the European Union*, *supra* note 21, at 11–14.
139. *See id.*
140. *See id.* at 5–16.
141. *See id.* at 5–6.
142. *See id.* at 9.
143. *See Cybersecurity Strategy of the European Union*, *supra* note 21 at 17–19; EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 17–24. The EU Strategy suggests a variety of other actions to achieve its cybersecurity priorities, including the creation of a single market for cybersecurity products, technical guidelines and recommendations, and the development of best practices to enhance cybersecurity policy. *See Cybersecurity Strategy of the European Union*, *supra* note 21, at 12–13.
144. *See* Holden, *supra* note 134.
145. *See infra* Part IV.A (discussing other global regulatory agencies).

economies."[146] A more recent study in 2012 reported that "[i]f [the Internet] were a national economy, it would rank in the world's top five, behind only the U.S., China, India, and Japan, and ahead of Germany."[147] Users access the Internet for banking, entertainment, news, technological innovation, education, and consumer shopping, among other things.[148] Businesses use networks internally to facilitate the exchange of information and to store consumer data.[149]

The Internet has accelerated economic growth in many countries through the diffusion of technology, increases in productivity, and opportunities for entrepreneurship and employment.[150] Conversely, cyberattacks on these systems are quite expensive.[151] Estimates of the cost of cybercrime vary, with recent reports estimating that the United States loses $100 billion each year in cybersecurity breaches.[152] Globally, those costs are estimated to be closer to $500 billion.[153] Thus, protecting access to the Internet and the integrity of networks is a significant economic concern for the international community.

Both strategies acknowledge the significance of the Internet to modern economies, but the United States and European Union diverge on the types and levels of economic regulation required in cybserspace.[154] The U.S. Strategy stresses the importance of preserving free trade and open markets in cyberspace and notes the reciprocal relationship between economic competition and innovation and the development of the Internet.[155] The U.S. Strategy can be interpreted, perhaps unsurprisingly, as suggesting a limited role for government—a

146. JAMES MANYIKA & CHARLES ROXBURGH, MCKINSEY GLOBAL INSTITUTE, THE GREAT TRANSFORMER: THE IMPACT OF THE INTERNET ON ECONOMIC GROWTH AND PROSPERITY 1 (2011).

147. Press Release, Boston Consulting Group, Clicks Grow Like BRICS: G-20 Internet Economy To Expand at 10 Percent a Year Through 2016 (Mar. 19, 2012), *available at http://www.bcg.com/media/PressReleaseDetails.aspx?id=tcm:12-100468.*

148. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 3.

149. *See* Christian Lanng, *Rethinking How You Use the Internet Is Crucial for Business Efficiency*, THE GUARDIAN (Apr. 23, 2013), http://www.theguardian.com/small-business-network/2013/apr/23/using-internet-business-owner.

150. DALBERG GLOBAL DEV. ADVISORS, OPEN FOR BUSINESS? THE ECONOMIC IMPACT OF INTERNET OPENNESS 27 (2014) *available at* http://www.dalberg.com/documents/Open_for_Business_Dalberg.pdf.

151. *See Cybercrime Costs May Reach $500 Billion, Study Estimates*, INDUSTRY WEEK, July 22, 2013, http://www.industryweek.com/technology/cybercrime-costs-may-reach-500-billion-study-estimates.

152. *Id.*

153. *Id.*

154. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 17–18; *Cybersecurity Strategy of the European Union*, *supra* note 21, at 2

155. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 17–18.

laissez-faire approach to cyberspace with the focus on individual economic and personal freedom.

Although the EU Strategy recognizes the important role of cybertechnology in the modern global economy,[156] the strategy addresses economic concerns chiefly in terms of cybercrimes, such as espionage and data theft.[157] In contrast to the U.S. Strategy, the EU Strategy does not discuss promoting open markets or improving free trade via cyberspace.[158] The EU Strategy does propose developing European markets for cybersecurity products and technological research and development.[159] In this context, however, the European market is a means to developing better tools for cybersecurity, rather than an end to be improved through strategic regulation.[160] The differing perspectives of the economic role of cyberspace, and the attendant differences of perspectives on regulation, indicate a strong potential for future international disagreement. With an increasingly global economy dependant on a completely global cyberspace,[161] consistency and centralization in cyberspace are necessary to successfully regulate and protect eocnomic interests.

C. Government Transparency and Individual Privacy

The third major concern underlying the need for global cybersecurity regulation is the principle of government transparency and individual privacy.[162] In 2013, revelations regarding the National Security Agency's ("NSA")[163] surveillance of electronic communications created significant privacy concerns among U.S. citizens.[164] The

156. *See Cybersecurity Strategy of the European Union*, *supra* note 21, at 2 (explaining that "[information technology] now underpins the complex systems which keep our economies running in key sectors such as finance, health, energy and transport; while many business models are built on the uninterrupted availability of the Internet and the smooth functioning of information systems").

157. *See id.* at 3.

158. *See id.* at 5–16.

159. *See id.* at 12–14.

160. *See id.* at 12–14.

161. *See* DALBERG GLOBAL DEV. ADVISORS, *supra* note 150, at 1–3.

162. This subsection focuses primarily on individual protection from government surveillance. Such surveillance is harmful for a variety of reasons, including its chilling effect on the exercise of civil liberties and the potential for discrimination and government coercion. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1936 (2013).

163. The National Security Agency is a U.S. intelligence agency charged with collecting signals intelligence. *Frequently Asked Questions About NSA*, NAT'L SEC. AGENCY CENT. SEC. SERV., https://www.nsa.gov/about/faqs/about_nsa.shtml (last updated Jan. 13, 2011).

164. JOHN W. ROLLINS & EDWARD C. LIU, CONG. RESEARCH SERV., RL43134, NSA SURVEILLANCE LEAKS: BACKGROUND AND ISSUES FOR CONGRESS 1–4 (2013).

allegations, leaked by former NSA employee Edward Snowden and later confirmed by the U.S. government, revealed a secret NSA program that collected "Internet communications and stored data of 'non-US persons' outside the US and those communicating with them."[165] Further leaks revealed that the NSA monitored the telephone communications of its allies, such as German Chancellor Angela Merkel and Brazilian President Dilma Rousseff.[166]

The revelations caused an international outcry and prompted a global conversation about the permissible boundaries of government surveillance of private citizens and the level of transparency and accountability required from government institutions.[167] In the months following the information leak, many countries denounced the NSA surveillance program.[168] A report released by the United Nations condemned such mass surveillance as "incompatible with existing concepts of privacy" because "[t]he communications of literally every Internet user are potentially open for inspection."[169]

The two strategies touch on the issue of government surveillance differently. The U.S. Strategy does not clearly address the issue of government surveillance, though references to "transparent governments"[170] and expanding government accountability[171] could be

165. Susan Landau, *Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations*, IEEE SECURITY & PRIVACY, July–Aug. 2013, at 54, 54 (noting that "[m]ore leaks followed, with details about the US government spying on Chinese computers [and] news that the NSA and its British counterpart GCHQ has used a monitored Internet café to eavesdrop on the communications of political leaders attending the 2009 G20 summit").

166. Susan Landau, *Highlights from Making Sense of Snowden, Part II: What's Significant in the NSA Revelations*, IEEE SECURITY & PRIVACY, Jan.–Feb. 2014, at 62, 62–63; *Embassy Espionage: The NSA's Secret Spy Hub in Berlin*, SPIEGEL ONLINE INTERNATIONAL (Oct. 27, 2013), http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html.

167. *See* Landau, *supra* note 166, at 63.

168. *Embassy Espionage: The NSA's Secret Spy Hub in Berlin*, *supra* note 166; Alissa J. Rubin, *French Condemn Surveillance by N.S.A.*, N.Y. TIMES (Oct. 21, 2013), http://www.nytimes.com/2013/10/22/world/europe/new-report-of-nsa-spying-angers-france.html?_r=1 ("French officials called the spying 'totally unacceptable' and demanded that it cease.").

169. Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, *Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, transmitted by Note of the Secretary-General*, ¶¶ 9, 18, U.N. Doc. A/69/397 (Sept. 23, 2014). Another report noted "the disturbing lack of governmental transparency associated with surveillance policies, laws and practices, which hinders any effort to assess their coherence with international human rights law and to ensure accountability." U.N. High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, ¶ 48, U.N. Doc. A/HRC/27/37 (June 30, 2014).

170. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 3.

171. *See id.* at 8.

broadly interpreted to condemn clandestine surveillance. Conversely, the EU Strategy explicitly rejects government surveillance of citizens in cyberspace.[172] However, unlike national security and economic concerns, the worrying differences are not simply between national strategies but between the official words of the strategies and the actions of the governments writing them.

Despite the implicit and explicit condemnations found in the strategies, both the United States, through the NSA, and various European Union member states, through their intelligence agencies, engage in the interception and sharing of data gathered over cyber networks.[173] This leaves open the question of whether individual cybersecurity strategies and regulations will be effective if disregarded by both their authors and other cyberspace actors. The inconsistencies and disagreements between the strategies on national security, economic, and privacy concerns indicate potential difficulty in regulating a borderless cyberspace through an individualized approach. Rather, the global community must come together to develop a consistent international cybersecurity regime to regulate an international cyberspace that affects them all.

IV. RESOLVING DIFFERENCES: A GLOBAL REGULATORY AGENCY

Although both the United States and the European Union advocate for international cooperation,[174] it may be difficult to align differing goals into a consistent cybersecurity regime through diplomacy and multilateral agreements alone.[175] Furthermore, recent allegations of government surveillance of electronic communications by the United States and European Union member states cast doubt on accountability and adherence of nations to self-created policies.[176] Meanwhile, cyberspace and its attendant threats are only predicted to grow, leading to greater interconnectedness and greater vulnerability.[177]

172. *See Cybersecurity Strategy of the European Union*, *supra* note 21, at 3, 15–16.

173. *See* ROLLINS & LIU, *supra* note 164, at 1–4; Julia Borger, *GCHQ and European Spy Agencies Worked Together on Mass Surveillance*, THE GUARDIAN, Nov. 1, 2013, http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden (describing electronic surveillance programs by German, French, Spanish, Swedish, and British intelligence agencies).

174. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 17–24; *Cybersecurity Strategy of the European Union*, *supra* note 21, at 13–16.

175. *See supra* Parts II–III.

176. *See supra* Part III.C (discussing recent allegations of government surveillance of citizens by the United States and European Union).

177. *See supra* Part II.C (explaining characteristics unique to cyberspace and their effects on cyberspace growth and vulnerability).

One solution to the problem of a fragmented cybersecurity regime is the creation of a global regulatory agency. This agency would be tasked with the development, implementation, and enforcement of a global cybersecurity regime. Specifically, this agency would address international cybercrime and suspected cyberwarfare in terms of prevention, investigation, and prosecution. Limiting the scope of the agency is necessary in order to provide the agency with a reasonable mandate and increase the likelihood of international accord. The international community must look to similar global regulatory regimes and current international cybersecurity efforts to structure a successful cybersecurity regulatory agency.

A. Blueprints for a Global Regulatory Agency

With governments, financial institutions, and individuals increasingly dependent on cybernetworks,[178] attacks, whether by criminals or states, can lead to devastating results.[179] A centralized response system will be better equipped to develop and control the potential weaponization of cyberspace, and such centralization is not unprecedented.[180] Indeed, the two most significant agreements between the U.S. and EU Strategies are an emphasis on international cooperation in the development of cybersecurity policy[181] and a commitment to adapting and applying existing norms and rules of law to cyberspace.[182] To guide the creation of a global agency for cyberspace regulation, the international community should look to its management of two previous threats to global welfare: chemical and nuclear weapons.

1. Organisation for the Prohibition of Chemical Weapons

The Organisation for the Prohibition of Chemical Weapons ("OPCW")[183] has successfully maintained international support for the

178. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 3.

179. *See* Landler & Markoff, *supra* note 4 (describing the effects of large-scale cyberattacks on Estonia).

180. *See infra* Part IV.A.1–2.

181. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 17–24; *Cybersecurity Strategy of the European Union*, *supra* note 21, at 5–16.

182. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 9; *Cybersecurity Strategy of the European Union*, *supra* note 21, at 15. In addition to major similarities, both strategies emphasize developing cybertechnology capabilities, increasing cyber resilience, and reducing cybercrime through domestic and international measures. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 18–20, 22–23; *Cybersecurity Strategy of the European Union*, *supra* note 21, at 5–14.

183. Alan Cowell, *Chemical Weapons Watchdog Wins Nobel Peace Prize*, N.Y. TIMES, Oct. 11, 2013, http://www.nytimes.com/2013/10/12/world/chemical-weapons-watchdog-wins-nobel-peace-prize.html.

regulation of chemical weapons.[184] The organization acts as a watchdog to help carry out the Chemical Weapons Convention ("CWC")[185] and sends inspectors to various signatory countries to ensure compliance.[186] The Chemical Weapons Convention itself is the product of over 60 years of international efforts to ban the use of poisonous weapons.[187] The member states of the OPCW represent roughly 98 percent of global population, landmass, and the worldwide chemical industry.[188]

The OPCW enjoys wide support and, in 2013, was awarded the Nobel Peace Prize.[189] In its announcement, the Nobel Committee praised the OPCW for its work in defining "the use of chemical weapons as a taboo under international law."[190] This "taboo-making" of a weapon or crime is incredibly powerful and should become the goal for regulating cyberspace. If cybercrime and cyberwar are treated as taboos because of their potentially debilitating effects, regulation and enforcement is more likely to be successful.

Although not necessarily life threatening, the destructive potential of cybercrime[191] likewise requires support for centralized action. The OPCW is an example of the potential for a mostly unified international response to the threat of global harm.[192] A global cybersecurity regulatory agency could similarly exist as a watchdog organization given power to enforce international law through a convention or treaty. Although cybercrime has not yet proven itself a grave enough threat to attract unified support for central regulation, its ever-increasing ubiquity may cause this to change.

---

184. *Id.*

185. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, Jan. 13, 1993, S. Treaty Doc. No. 103-21, 1974 U.N.T.S. 317.

186. Cowell, *supra* note 183 (describing the aims of the Chemical Weapons Convention: "to destroy all chemical weapons under international verification, to prevent the creation of new chemical weapons, to help countries protect themselves against chemical attack, and to foster international cooperation in the peaceful use of chemistry").

187. Michael P. Scharf, *Clear and Present Danger: Enforcing the International Ban on Biological and Chemical Weapons Through Sanctions, Use of Force, and Criminalization*, 20 MICH. J. INT'L L. 477, 479–85 (1999). The CWC followed a long string of failed or limited attempts to ban such weapons, including the Hague Convention of 1907, the Geneva Protocol of 1925, and the Biological Weapons Convention of 1972. *Id.*

188. *OPCW Member States*, ORG. FOR THE PROHIBITION OF CHEMICAL WEAPONS, http://www.opcw.org/about-opcw/member-states/ (last visited Mar. 30, 2015).

189. Cowell, *supra* note 183.

190. Press Release, The Norwegian Nobel Committee, The Nobel Peace Prize for 2013 (Oct. 11, 2013).

191. *See* Broad, Markoff & Sanger, *supra* note 15, (discussing the damage sustained by the Iranian nuclear program as a result of Stuxnet).

192. *See* Cowell, *supra* note 183.

2. International Atomic Energy Association

Another example of global regulation of potentially dangerous technology is the International Atomic Energy Agency ("IAEA").[193] The IAEA is "the world's centre for cooperation in the nuclear field" and works "to promote the safe, secure and peaceful use of nuclear technologies."[194] Established in 1957 as an independent organization related to the UN,[195] the IAEA has 164 member states and is based on the 1956 IAEA statute.[196]

One of the most important functions of the IAEA is its establishment and enforcement of nuclear safety standards through "its reporting system, site inspections, and safety assistance programs."[197] Although the IAEA can apply its regulatory and enforcement powers only when a state agrees to receive IAEA assistance, it remains incredibly influential in developing international standards for nuclear energy use.[198] Indeed, like the OPCW, the IAEA and its Director General at the time, Mohammad ElBaradei, were jointly awarded the Nobel Peace Prize 2005.[199] The Nobel Committee noted that despite increasing nuclear threats, the IAEA represents international cooperation in ensuring that nuclear energy is used for peaceful purposes.[200] Further, the IAEA has played a significant role in establishing five international nuclear safety conventions in order to harmonize international standards and create a centralized body of nuclear regulations.[201] A global cybersecurity agency could draw on the structure and work of the IAEA as a template. The voluntary nature of IAEA regulation and enforcement and the difficulties of preventing the increase of nuclear threats may provide the architects of a global cybersecurity agency with examples of methodology as well as potential obstacles.

193. *Atoms for Peace*, INT'L ATOMIC ENERGY AGENCY, https://www.iaea.org/about (last visited Mar. 28, 2015).

194. *The "Atoms for Peace" Agency*, INT'L ATOMIC ENERGY AGENCY, https://www.iaea.org/about/about-iaea (last visited Mar. 28, 2015).

195. *Id.*

196. *See Member States of the IAEA*, INT'L ATOMIC ENERGY AGENCY, https://www.iaea.org/about/memberstates (last visited Mar. 28, 2015); DAVID FISCHER, HISTORY OF THE INTERNATIONAL ATOMIC ENERGY AGENCY: THE FIRST FORTY YEARS 33–35 (1997).

197. Karen McMillan, Note, *Strengthening the International Legal Framework for Nuclear Energy*, 13 GEO. INT'L ENVTL. L. REV. 983, 990 (2001).

198. *Id.*

199. Press Release, The Norwegian Nobel Committee, The Nobel Peace Prize for 2005 (Oct. 7, 2005).

200. *Id.*

201. *See* McMillan, *supra* note 197, at 990–94.

B. *Current Support for a Global Response*

Many aspects of such an agency already exist in part.[202] While neither the United States nor the European Union has indicated a willingness to create any type of centralized cyberspace regulation yet,[203] both support the Convention on Cybercrime[204] and harmonizing international cybercrime laws.[205] Indeed, the Convention on Cybercrime already addresses many challenges presented by international cybercrime, including jurisdiction, extradition, and procedural powers for investigation and prosecution.[206]

Although the Convention on Cybercrime applies chiefly to European countries,[207] its framework for the harmonization of cybercrime law among signatories could be used as a template for another international treaty on cybercrime and cyberwar. Similarly, the Global Agenda[208] advocates and establishes a plan for harmonization and the development of a consistent international cybersecurity framework.[209] As an initiative of the ITU, the Global Agenda, through IMPACT, is open to assist any of the ITU's 193 member states and as of 2011 has the support of 137 countries.[210] These existing international agreements, coupled with the U.S. and EU Strategies' spirit of international cooperation,[211] indicate international support for some global regulation. Indeed, a growing user of cyberspace, China, recently indicated support for international cyberregulation.[212]

---

202. *See supra* Part II.D, for a discussion of the current international cybersecurity regime.

203. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 9, 22; *Cybersecurity Strategy of the European Union*, *supra* note 21, at 17.

204. *See supra* Part II.D.2 (discussing the Convention on Cybercrime in detail).

205. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 19–20; *Cybersecurity Strategy of the European Union*, *supra* note 21, at 15.

206. *See Council of Europe Convention on Cybercrime*, *supra* note 127, at ch. II–III.

207. *See* Council of Eur., *supra* note 109 (indicating that the Convention on Cybercrime is open to members of the Council of Europe and only a few non-members including the United States, Argentina, and South Africa).

208. *See supra* Part II.D.1 (discussing the development of the Global Agenda and its goals).

209. *See Global Cybersecurity Agenda*, *supra* note 98, at 10.

210. *International Multilateral Partnership Against Cyber Threats*, *supra* note 99, at 4–5.

211. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 17–24; *Cybersecurity Strategy of the European Union*, *supra* note 21, at 13–16.

212. Ananth Krishnan, *After Snowden Revelations, China Calls for Cyber Security Regulations*, THE HINDU, June 14, 2013, http://www.thehindu.com/news/international/after-snowden-revelations-china-calls-for-cyber-security-regulations/article4814104.ece.

C. *Structuring a Global Cybersecurity Regulatory Agency*

A global cybersecurity regulatory agency would have two main points of focus: cybercrime and cyberwar. Cybercrime issues include conflicts of laws, jurisdiction, investigation, and extradition, among other things.[213] Cyberwar issues include global agreement on the limitations of the weaponization of cyberspace, diplomacy, and enforcement.[214]

Perhaps most importantly, the agency would require an international treaty outlining its scope and regulatory and enforcement powers. Both the OPCW and the IAEA are rooted in international agreement manifested through treaty or statute.[215] The Convention on Cybercrime already addresses many of the issues of the cybercrime branch of a regulatory agency.[216] A companion treaty delineating international law on cyberwar could form the foundation for the regulatory agency.

In terms of structure, the UN provides a natural home for a global regulatory agency.[217] There, it could work closely with related UN structures such as the ITU.[218] A possible inspiration for a blueprint of the agency itself is the newly established Cybercrime Centre.[219] Its multifaceted functions as an independent information hub, training center, and investigation resource[220] could be replicated and expanded to apply beyond the borders of Europe. Such an agency could act as a hub for interaction between law enforcement agencies such as Interpol[221] and the Central Intelligence Agency (CIA).[222] It would also facilitate international coordination of cybercrime detection and investigations.

---

213. *See supra* note 206 and accompanying text (describing issues covered by the Convention).

214. *See generally* Hathaway et al., *supra* note 8.

215. *See supra* Part IV.A.1–2.

216. *See supra* Part II.D.2 (discussing the Convention).

217. *See* ITU Constitution and Convention, *supra* note 94, at 24 (discussing the ITU's position as a UN specialized agency, where it encourages cooperation in developing telecommunication technology regulation).

218. *See supra* Part II.D.1 (explaining the structure and purpose of the ITU and its place in the existing international cybersecurity regime).

219. *See supra* Part II.D.4 (discussing the structure and functions of the Cybercrime Centre).

220. *See* Zagaris, *supra* note 114.

221. *See Overview*, INTERPOL *http://www.interpol.int/About-INTERPOL/Overview* (last visited Feb. 11, 2015); *see also* Patricia E. Apy, *Current International and Domestic Issues Affecting Children: Managing Child Custody Cases Involving Non-Hague Contracting States*, 14 J. AM. ACAD. MATRIMONIAL L. 77, 89 (1997) (describing Interpol as an organization coordinating law enforcement and mutual assistance between its member nations).

222. *See About CIA*, CENTRAL INTELLIGENCE AGENCY (Apr. 19, 2013), https://www.cia.gov/about-cia; *see also* Daniel L. Pines, *CIA & NSA: The Continuing Viability of* Totten v. Unites States, 53 ADMIN L. REV. 1273, 1277 (2001) (describing the origins and functions of the CIA).

The agency could use the examples of the OPCW and IAEA to create effective procedures for regulation. Indeed, countless methods and structures for effective regulation exist, and the international community has the ability to create an agency that would best suit the needs of global users of cyberspace.

Although the scope and effects of cybersecurity threats are global,[223] neither the U.S. nor EU Strategy currently proposes centralized regulation.[224] The EU Strategy goes so far as to reject the notion of centralized supervision because of the complexity of issues and actors.[225] However, support for centralized regulation may increase as both cyberspace and cybersecurity threats become more pervasive.[226] Like Aesop's well-prepared Ant,[227] developing a global regulatory system now may greatly benefit society in the future.

CONCLUSION

Cyberspace is a growing and evolving international medium of communication. Individuals, businesses, and governments increasingly depend on cybertechnology to complete countless daily tasks and operations. This dependence has resulted in the storage of large amounts of personal and official data in information system networks, requiring the protection of cybersecurity measures. Unfortunately, as cyberspace grows, so do potential cybersecurity risks and vulnerabilities. The unique nature of cyberspace poses challenges to regulation and enforcement in cyberspace.

In response to these problems, the international community has developed a piecemeal cybersecurity regime, and the United States and European Union have contributed to this regime with individual cybersecurity strategies. However, the disagreements between the two strategies indicate that effective regulation may prove difficult to achieve. Currently, there is no global regulatory agency to regulate international cybercrime. As cybersecurity risks increase, however, the need for a global regulatory agency will become more evident. Regardless of the form of the global regulatory agency, the potential costs of large-scale cyberattacks, both economic and personal, should

223. *Cybersecurity Strategy of the European Union*, *supra* note 21, at 9.

224. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 22, at 8–12 (discussing various options for international cybersecurity development but omitting the possibility of centralized regulation); *Cybersecurity Strategy of the European Union*, *supra* note 21, at 17.

225. *Cybersecurity Strategy of the European Union*, *supra* note 21, at 17.

226. *See supra* Part II.

227. *See* AESOP, AESOP'S FABLES 146 (V.S. Vernon Jones trans., Barnes & Noble Classics 2003).

convince the international community to centralize its cybersecurity efforts.