insights

American Society of International Law

June 8, 2011 Volume 15, Issue 15

International Law and the Future of Cyberspace: The Obama Administration's *International Strategy for Cyberspace*

By David P. Fidler

Introduction

On May 16, 2011, the Obama Administration released its *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*.[1] President Obama stated that the *International Strategy* represents "the first time that our Nation has laid out an approach that unifies our engagement with international partners on the full range of cyber issues."[2] In shaping an approach to maximize the benefits of cyberspace and mitigate the threats to its expanded use, the Obama Administration emphasizes the need for "building the rule of law"[3] through international norms and processes. This *Insight* describes the *International Strategy* and the role the Obama Administration constructs for international law in its vision of the future of cyberspace.

The *International Strategy*

Background

Since widespread personal, commercial, and governmental use of the Internet began in the mid-1990s, U.S. administrations have attempted to facilitate use of cyberspace and protect users from malevolent activities. During this period, the Internet became increasingly important to social, economic, and political life around the world, but threats, such as cyber-crime, expanded as well. Concerns mounted about the ineffectiveness of U.S. approaches to protect cyberspace, exemplified by a December 2008 report, which argued that "America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration."[4] Upon taking office, the Obama Administration conducted a cyberspace policy review, which concluded that "[t]hreats to cyberspace pose one of the most serious economic and national security challenges of the 21st Century for the United States and our allies."[5]

Security was not, however, the only concern about the future of cyberspace. The growing

RELATED ASIL INSIGHTS

The Google Book Settlement and International Intellectual Property Law

Google, China, and Search

WTO Panel Report on Consistency of Chinese Intellectual Property Standards

Insights Archive>>

DOCUMENTS OF NOTE

International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World

CSIS Commission on Cybersecurity for the 44th Presidency, Securing Cyberspace for the 44th Presidency

Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure

G8 Declaration on Renewed Commitment for Freedom and Democracy

ASIL EISIL>>

ORGANIZATIONS OF NOTE

U.S. Department of State

U.S. Department of Defense

U.S. Strategic Command

U.S. Cyber Command

U.S. White House

The purpose of ASIL Insights is to provide concise and informed background for developments of interest to the international community. The American Society of International Law does not take positions on substantive issues, including the ones discussed in this Insight. Educational and news media

Security was not, however, the only concern about the future of cyberspace. The growing rivalry between the United States and China increasingly highlighted distinct attitudes about the meaning of cyberspace and the purpose of the Internet. The Obama Administration set out to establish its normative perspective for cyberspace as a global political space, with Secretary of State Hillary Clinton's January 2010 speech on "Internet Freedom" as a centerpiece of this effort.[6] Secretary Clinton stated, "We stand for a single internet where all of humanity has equal access to knowledge and ideas."[7] Achieving this goal, she asserted, requires advancing freedom of expression and worship and freedom from fear and want. This "Internet freedom" agenda gained traction in the wake of the perceived utility of the Internet during the democratic uprisings in North Africa and the Middle East in first half of 2011. In short, the Obama Administration saw opportunities to imprint an ideology on the possibilities technology created for peoples around the world.

Purpose, principles, and policy pathways

In the *International Strategy*, the Obama Administration attempts to integrate economic, security, and political strands of U.S. policy on cyberspace into an overarching, coherent strategic approach. This approach seeks to advance the social, economic, and political advantages a networked world creates for individuals, communities, and nations while addressing threats that undermine the Internet's value for communications, commerce, and international cooperation. Guiding this task are "core commitments to *fundamental freedoms, privacy,* and the *free flow of information*."[8] The *International Strategy* recognizes the age-old tension between security and liberty in pushing for greater cybersecurity and expanded Internet freedoms, but it argues that, through the "rule of law," its approach "supports our national security and advances our common values."[9]

The *International Strategy* seeks to ensure that cyber-technologies are open, interoperable, secure, reliable, and stable.[10] Pursuing these objectives globally requires the United States to engage in integrated efforts through diplomacy, defense, and development policies.[11] The *International Strategy* is a "roadmap" for U.S. government agencies "to better define and coordinate their role . . . to execute a specific way forward, and to plan for future implementation."[12] To support such activities, the *International Strategy* organizes U.S. government endeavors "across seven interdependent areas of activity, each demanding collaboration within our government, with international partners, and with the private sector"[13] (see Table 1).

Table 1. Seven U.S. Government Areas of Activity under the *International Strategy*

Economy: promoting international standards and innovative open markets

Protecting our networks: enhancing security, reliability, and resiliency

Law enforcement: extending collaboration and the rule of law

Military: preparing for 21st century security challenges

Internet governance: promoting effective and inclusive structures

International development: building capacity, security, and prosperity

Internet freedom: supporting fundamental freedoms and privacy

International Law and the *International Strategy*

The "rule of law" in cyberspace

A theme running through the *International Strategy* is the need for the "rule of law" in cyberspace governance domestically and internationally. It defines the rule of law as "a civil order in which fidelity to laws safeguards people and interests; brings stability to global markets; and holds malevolent actors to account internationally[.]"[14] Given the challenges confronting cyberspace, this fidelity to law requires establishing "an environment of expectations, or norms of behavior" that builds "a consensus on what constitutes acceptable behavior, and a partnership among those who view the functioning of these [cyber-]systems as essential to the national and collective interest."[15]

Substantive international legal norms

International law and legal processes play critical roles in the Obama Administration's vision of prosperity, security, and openness in a networked world. In terms of substantive law, the *International Strategy* makes clear that many existing principles of international law operating in times of peace and conflict also apply in cyberspace. These existing international legal rules include respect for the fundamental civil and political rights of freedom of expression and association, privacy, and property; state responsibility to deny criminals safe haven; and the right to use force in individual or collective self-defense in response to armed attacks.[16]

The *International Strategy* also recognizes that "unique attributes of networked technology" mean that (1) more clarity is needed on how existing international legal norms operate in cyberspace; and (2) new norms are required.[17] Emerging cyber-specific norms requiring development and implementation include:

- *Global interoperability*: ensuring end-to-end operability of an Internet accessible to all;
- *Network stability*: respecting free flow of information in national networks and avoiding arbitrary interference with internationally connected infrastructure;
- *Reliable access*: no arbitrary deprivation or disruption of individual access to the Internet and other networked technologies;
- *Multi-stakeholder governance*: Internet governance must include all appropriate stakeholders and not just governments; and
- *Cybersecurity due diligence*: state responsibility to protect information infrastructures and to secure national systems from misuse or damage.[18]

International legal processes

In addition to focusing on existing and emerging substantive international norms, the *International Strategy* emphasizes that achieving the rule of law for cyberspace demands international cooperation, asserting that such cooperation "is a first principle."[19] This theme is particularly strong in the embrace of strengthened international partnerships that can "build consensus around principles of responsible behavior in cyberspace and the actions necessary . . . to build a system of cyberspace stability."[20] The broad vision of cyberspace's future and the diversity of international rules and norms affected will require cooperation in many processes and venues (e.g., economic, law enforcement, military, development, and human rights), supplemented by implementation of the emerging principle of multi-stakeholder governance.

Potential problems

Despite acknowledging the importance of existing international legal rules, the *International Strategy* never mentions two basic principles affected by its content—respect for sovereignty and non-intervention in the domestic affairs of other states. The intent to achieve Internet freedom globally by supporting "civil society actors in achieving reliable, secure, and safe platforms for freedoms of expression and association"[21] targets governments that do not, on or off line, respect free speech and democratic politics. The Obama Administration's cyber-support for democracy movements suggests that the *International Strategy* does not tolerate pluralism in cyberspace concerning human rights and domestic forms of governance.[22] To express importance given to diplomacy, defense, and development, the *International Strategy* adds a fourth "d"—democracy. This purpose will create concerns for non-democratic countries attached to the principles of sovereignty and non-intervention.

The ideological thrust of the *International Strategy* raises questions about the emphasis on international cooperation and consensus building. First, important players with power to shape how cyberspace functions, especially China, might take positions that produce consensus on the lowest common denominator, creating agreement only on superficial principles of responsible behavior in cyberspace. Second, the substantive norms in which the Obama Administration anchors the *International Strategy*, especially those civil and political rights informing the idea of Internet freedom, appear to be non-negotiable from the U.S. perspective. This position undermines the claim that the United States wants to negotiate new norms for cyberspace. To other countries, the U.S. position might appear to be an offer to negotiate how the U.S. vision gets implemented globally, which could produce difficulties in diplomatic processes that have to address cyberspace challenges.

Impact and Implementation

International law and the new geo-cyberpolitics

International law operates within a context shaped by larger political trends and tensions, and this geo-political reality affects the role of international law in cyberspace governance. The *International Strategy* represents the Obama Administration's statement of principles that connects to earlier assertions of U.S. cyber-power, particularly the establishment in 2010 of the U.S. Cyber Command—a specific military combatant command dedicated to the development and deployment of "full spectrum" U.S. military cyber-capabilities.[23] This alignment of U.S. principle and power concerning the future of cyberspace arises strategically from rival cyber concepts and capabilities held foremost by China. The *International Strategy* sketches U.S. doctrine to guide the country in the intensifying competition over what cyberspace should be and how it should function. In this realm of geo-cyberpolitics, the rival sides will employ international law differently to justify their divergent positions.

The G8 declaration and the Internet

The Obama Administration's understanding of the *International Strategy*'s normative and geo-political importance appeared in the G8 declaration from the summit in Deauville, France, at the end of May 2011. The *International Strategy* stated that the shaping "cyberspace norms of behavior must begin with clear agreement among like-minded countries."[24] In keeping with this view, the G8 Declaration on Renewed Commitment to Freedom and Democracy included a section on the Internet echoing the *International Strategy*, including insistence that the Internet's use must include "respect for the rule of law, human rights and fundamental freedoms, [and] the protection of intellectual property rights, which inspire life in every democratic society for the benefit of all citizens."[25]

U.S. government implementation of the International Strategy

The *International Strategy* will guide development of more specific U.S. government plans. For example, the Department of Defense is expected to release its formal strategy document in the near future.[26] Given concerns experts have raised about the *International Strategy*'s lack of detail on how it will be implemented,[27] the agency-specific plans will constitute important benchmarks, including how international law features in specific U.S. government implementation activities.

About the Author:
David P. Fidler, an ASIL member, is the James Louis Calamaras Professor of Law and a Fellow at the Center for Applied Cybersecurity Research at Indiana University.

Endnotes:

[1] White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World(May 2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [hereinafter *International Strategy*].

[2] *Id*. at i.

[3] *Id*. at 3.

[4] Ctr. on Strategic and Int'l Studies [CSIS], Commission on Cybersecurity for the 44th Presidency, Securing Cyberspace for the 44th Presidency 11 (Dec. 2008), *available at* http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

[5] White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure 1 (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

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

[7] *Id*.

[8] *International Strategy, supra* note 1, at 5 (emphasis in original).

[9] *Id*.

[10] *Id*. at 8-11.

[11] *Id*. at 11-15.

[12] *Id*. at 25.

[13] *Id*. at 17.

[14] *Id*. at 5.

[15] *Id*. at 9.

[16] *Id*. at 10.

[17] *Id*. at 9.

[18] *Id*. at 10.

[19] *Id*. at 8.

[20] *Id*. at 11.

[21] *Id*. at 23.

[22] *See, e.g.,* Mark Landler & Brian Knowlton, *U.S. Policy to Address Internet Freedom*, N.Y. Times, Feb. 14, 2011, *available at* http://www.nytimes.com/2011/02/15/world/15clinton.html.

[23] William J. Lynn III, *Introducing U.S. Cyber Command,* Wall Street J., June 3, 2010, *available at* http://online.wsj.com/article/SB10001424052748704875604575280881128276448.html.

[24] *International Strategy, supra* note 1, at 12.

[25] G8 Declaration on Renewed Commitment for Freedom and Democracy art. II, § 10, May 27, 2011, *available at* http://www.g20-g8.com/g8-g20/g8/english/news/news/renewed-commitment-for-freedom-and-democracy.1314.html.

[26] Siobhan Forman & Julian E. Barnes, *Cyber-Combat: Act of War—Pentagon Sets Stage for U.S. to Respond to Computer Sabotage with Military Force,* Wall Street J., May 31, 2011, *available at* http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html?mod=googlenews_wsj.

[27] *See, e.g.,U.S. Global Cybersecurity Plan Falls Short, Experts Warn*, Huffington Post.com, May 17, 2011, *available at* http://www.huffingtonpost.com/2011/05/17/us-global-cybersecurity-plan-falls-short_n_863321.html.