insights

American Society of International Law

June 20, 2012 Volume 16, Issue 22

Recent Developments and Revelations Concerning Cybersecurity and Cyberspace: Implications for International Law

By David P. Fidler

Introduction

In recent weeks, media reports have addressed actions, discoveries, and controversies relating to cybersecurity and cyberspace that have implications for international law, including war, espionage, terrorism, and crime in cyberspace and the architecture and governance of the Internet. This *Insight* describes these episodes and analyzes their importance for the relationship between international law and cybersecurity and cyberspace.

Developments and Revelations Concerning Cybersecurity and Cyberspace

Origins of Stuxnet

On June 1, 2012, David Sanger of the *New York Times* reported that the United States and Israel developed the Stuxnet computer worm and used it to attack Iran's uranium enrichment facilities.[1] When discovered in 2010, experts considered Stuxnet to be a "game changing" cyber weapon because of its complexity, purpose, and performance. The Stuxnet worm exploited unknown vulnerabilities in Windows software,[2] targeted industrial control systems at Iran's enrichment facilities,[3] and reportedly damaged over 1,000 centrifuges and disrupted Iran's enrichment efforts.[4] The complexity and nature of the attack led many to suspect that a state, most likely the United States and/or Israel, created Stuxnet. Sanger appeared to confirm this suspicion, revealing that the Stuxnet project, code-named "Olympic Games," began during the George W. Bush administration and accelerated under President Barack Obama.[5]

The Flame Virus

In late May 2012, experts discovered a computer virus dubbed "Flame."[6] Unlike Stuxnet, Flame operated as an espionage tool because it infiltrated computers and exfiltrated

RELATED ASIL INSIGHTS

The Internet, Human Rights, and U.S. Foreign Policy: The Global Online Freedom Act of 2012

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

Protecting Children from Cyber Crime: The Twentieth Session of the UN Commission on Crime Prevention and Criminal Justice

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 Telecommunication Regulations

Council of Europe Convention on Cybercrime

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

ASIL EISIL>>

ORGANIZATIONS OF NOTE

International Telecommunications Union

Internet Society

U.S. Department of State

U.S. House of Representatives

U.S. Senate

information from them. As such, experts believe that a government or governments created Flame to spy on other countries. This large and complex virus was predominantly found in computers in the Middle East, with Iran being particularly affected. Some information indicated that Flame had been operating for years before detection and shared some code with early versions of Stuxnet.[7] The Iran and Stuxnet aspects encouraged speculation that the United States and/or Israel were responsible for Flame.[8] Although cyber espionage is not a new problem,[9] Flame garnered international attention, including an alert from the International Telecommunications Union ("ITU") and assertion by the ITU's cybersecurity coordinator that Flame constituted "a much more serious threat than Stuxnet."[10]

U.S. Cyber Activity Against Al-Qaeda Web Sites

On May 23, 2012, Secretary of State Hillary Clinton described U.S. efforts to alter information on web sites used by al-Qaeda's affiliate in Yemen.[11] This State Department-led, interagency activity sought to discredit terrorist use of the Internet. Terrorists have not demonstrated interest in launching cyber attacks, but they use the Internet for recruiting and other purposes. Although described in press reports as "hacking" or "cyber war,"[12] the State Department apparently altered and re-posted recruiting ads that appeared on al-Qaeda web sites in ways that described the toll al-Qaeda has inflicted on Yemen's people—actions that probably did not require hacking into or attacking computers.[13] Government-sponsored actions against terrorist web sites have occurred before,[14] but Secretary Clinton's description of a State Department-led strategy that includes altering information on terrorist web sites potentially revealed a more open, coordinated, and forward-leaning U.S. approach to cyber counter-terrorism.

Global Transition to Internet Protocol Version 6

On June 6, 2012, the Internet Society—a global non-governmental organization dedicated to promoting the open development and use of the Internet—sponsored the "World IPv6 Launch," an effort to have major Internet service providers and web companies accelerate the transition from Internet Protocol version 4 ("IPv4") to Internet Protocol version 6 ("IPv6").[15] Internet communications occur through the Transmission Control Protocol/Internet Protocol ("TCP/IP") standard, which controls how data is organized, addressed, transmitted, and received on the Internet. The "Internet Protocol" provides the addressing system for sending information over the Internet. As with other Internet protocols, the non-governmental Internet Engineering Task Force ("IETF") developed IPv6.[16]

Internet experts believe IPv6 is critical because growth in Internet usage has exhausted the number of addresses IPv4 had available (approximately 4.3 billion).[17] IPv6 increases the number of addresses to approximately 340 undecillion (or trillion, trillion, trillion), making exhaustion of addresses virtually impossible.[18] IPv6 will ensure that the Internet can handle growth in future use. Although IPv6 solves the Internet address problem, it has raised questions about its potential impact on cybersecurity, ranging from claims that IPv6 will provide greater online security and help law enforcement address cyber crimes[19] to concerns that IPv6 might benefit cyber criminals and governments seeking to repress political dissent.[20]

Internet Governance Controversy

In May 2012, controversy intensified about the December 2012 meeting of the ITU's World Conference on Telecommunications ("WCIT").[21] WCIT delegates will consider revising the

International Telecommunication Regulations (“ITR”), a treaty adopted by ITU member states.[22] Some countries want significant changes to the ITR, including potentially expanding the ITU’s role with respect to Internet governance.[23] Moving in this direction would require shifting Internet governance from multi-stakeholder, non-governmental mechanisms, such as the Internet Society, IETF, and Internet Corporation for Assigned Names and Numbers (“ICANN”), to the inter-governmental ITU. The Obama administration, members of Congress, and stakeholders in the current governance system oppose attempts to centralize Internet governance in an inter-governmental forum for many reasons, including perceived threats from governance centralization to Internet innovation and freedom. The WCIT controversy represents the latest flare-up about Internet governance, with similar disagreements appearing during the ITU’s World Summit on the Information Society (2003-2005).[24]

Implications for International Law

Cybersecurity and International Law

These developments and revelations underscore the expanding importance of cyberspace and cybersecurity in international relations. Stuxnet, Flame, and U.S. actions against al-Qaeda web sites demonstrate deepening interest in the utility of cyber technologies to achieve national security objectives, including armed conflict, covert sabotage, espionage, and counter-terrorism. Like previous advances in communication technologies, states are harnessing the Internet for security needs as opposed to treating cyberspace as a unique political domain. How well existing rules of international law apply to such security-driven behavior is important to explore. This question is not new, but developments, such as Stuxnet and Flame, renew debates about the application of international law to cybersecurity problems.

With respect to cyber espionage, the lack of international law on espionage[25] means that Flame and other state-crafted spyware operate without international regulation. The ubiquity of cyber espionage suggests that no consensus exists among states to change this reality, which replicates what happened with every new technology adapted for spying. Unless states begin to perceive cyber espionage as an atypical danger to national security and international order, international law is unlikely to gain traction in this area, no matter how many headlines Flame or future spyware produces.

In terms of Stuxnet, attribution of this cyber attack to the United States and Israel does not answer international legal questions about this episode. To analyze Stuxnet under international law requires characterizing what this incident means in legal terms. Commentators have often described Stuxnet in terms of “cyber war,”[26] but governments have not yet responded to Stuxnet (before or after revelations about its origins) as if it constituted an illegal use of force or armed attack or a legal use of force in self-defense. If state use of a cyber weapon designed to damage property is neither a use of force nor armed attack, then how should international lawyers characterize it? Stuxnet is only one incident, so state practice might lack clarity for many reasons. However, even with the problem of attribution resolved, international lawyers confront the problem of how to apply international law on the use of force to cyber weapons and cyber attacks after Stuxnet.

The international legal significance of the U.S. government’s alterations to propaganda on al-Qaeda web sites relates to questions about what cyber counter-terrorism might involve in the future. What the State Department accomplished does not appear to violate

international law applicable to counter-terrorism. However, will integration of cyber technologies with counter-terrorism strategies lead to more aggressive use of such technologies against terrorist organizations, and, if so, what would such use mean under international law? Some might not consider this question significant because U.S. counter-terrorism already involves aggressive and controversial use of lethal weapons against terrorists deployed from drones or by special operations forces. More aggressive use of cyber technologies against terrorists is unlikely to cause the political and legal notoriety non-cyber U.S. counter-terrorism strategies have generated.

Cyberspace and International Law

The transition of Internet architecture to IPv6 is important to ensuring that the Internet maintains sustained growth—a significant achievement globally for political, economic, and social reasons. And, it is an achievement that owes little, if anything, to international law. IPv6 has been developed, supported, and largely implemented by non-state actors operating without reference to treaties or rules of customary international law. With the transition to IPv6 still underway, assessing how adoption of IPv6 might affect security, privacy, and human rights in cyberspace is difficult, which complicates exploring IPv6's implications for international law. Certainly, if IPv6 produces security benefits through technological advances, it will mitigate perceptions that new international legal tools or initiatives are needed for cybersecurity problems, such as cyber crime.

Possible negative externalities of IPv6 adoption, such as providing new opportunities for cyber crime or repressive governments to undermine privacy and Internet freedom, could affect international law. Many experts consider international legal instruments relevant to cyber crime, such as the Council of Europe's Convention on Cybercrime,[27] ineffective and inadequate.[28] If cyber criminals find the IPv6 environment as or more conducive to cyber crime than IPv4, then existing international law on cyber crime might become more suspect, possibly falling into disrepute. Similarly, if IPv6 permits governments to attribute Internet activity more readily to specific devices and persons, this outcome might adversely affect enjoyment of Internet-relevant human rights protected by international law, including the rights to privacy, freedom of expression, and freedom of association.

The WCIT controversy involves international law in the form of the ITR—a binding treaty adopted in 1988, before the Internet became a global phenomenon. Proposals to amend the ITR to take account of the Internet's importance could seek to bring more of what is now governed in a decentralized manner largely by non-governmental organizations, such as IETF and ICANN, within formal international law. Some countries have expressed dissatisfaction with the status quo, arguing that it does not respond to their needs and permits the United States to influence Internet governance disproportionately. For example, in June 2011, Russian Prime Minister Vladimir Putin stated a desire to establish "international control over the Internet, using the monitoring and supervisory capabilities of the International Telecommunication Union."[29]

In response to fears that WCIT would change Internet governance, the U.S. House of Representatives declared on May 30, 2012, its concern about proposals that "would justify under international law increased government control over the Internet and would reject the current multistakeholder model that has enabled the Internet to flourish[.]"[30] Similarly, in congressional hearings on May 31, an Internet Society policy official argued that "it is not clear . . . that the international treaty making process represents the most effective way to manage cross-border Internet communications, or that some of the proposals currently

being floated are consistent—or even compatible—with the multistakeholder model of Internet governance that has emerged over the past 15 years."[31]

Leaks in early June 2012 of ITU documents being prepared for WCIT produced skepticism about the alleged ITU "takeover" of Internet governance and the argument that "the real conflict is not over governance of the Internet . . . but over the division of the spoils, with international telecommunications operators [within countries] trying to use the I.T.U. to extract revenue from American Internet companies."[32] In this contentious context, what ITR changes member states of the ITU can negotiate in December 2012 remains to be seen.

Conclusion

Analyses of cybersecurity and cyberspace often involve doubts about the applicability and effectiveness of international law. Information about Stuxnet's origins and discovery of Flame reinforce these doubts because they highlight the lack of international law (as with cyber espionage) and uncertainty in its application (as with Stuxnet). Nothing about the Stuxnet or Flame revelations suggests that states, especially the great powers and, in particular, those concerned about U.S. cyber power, will scale back cyber espionage activities or development of offensive and defensive cyber capabilities—a situation not conducive to developing international legal rules on cybersecurity challenges. Uncertainty whether IPv6 might benefit cyber criminals and repressive governments focuses attention on the ineffectiveness of existing international legal instruments on cyber crime and on cyber-facilitated human rights. Negotiations on revising the ITR reveal the unimportance of international law to existing Internet architecture and governance and the difficulties facing efforts to change the status quo through new international legal rules. These developments and revelations suggest that international law's role in shaping what the Obama administration has called "norms of responsible behavior in cyberspace"[33]will be fraught with difficulties for the foreseeable future.

About the Author:
David P. Fidler, an ASIL member, is the James Louis Calamaras Professor of Law at the Indiana University Maurer School of Law, and is a Fellow at the Indiana University Center for Applied Cybersecurity Research. He thanks Lesle Conway and Patrick LaMondia for research assistance.

Endnotes:

[1] David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. Times, June 1, 2012, at A1.

[2] Nicolas Falliere, Liam O. Murchu & Eric Chien, *W.32 Stuxnet Dossier* (Version 1.4, Feb. 2011), *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[3] *Id.*

[4] Sanger, *supra* note 1, at A1.

[5] *Id.*

[6] Thomas Erdbrink, *Iran Confirms Attack by Virus That Collects Information*, N.Y. Times, May 29, 2012, at A4.

[7] Kim Zeiter, *Researchers Connect Flame to US-Israel Stuxnet Attack*, Wired.com (June 11,

2012), *available at* http://www.wired.com/threatlevel/2012/06/flame-tied-to-stuxnet/?utm_source=June+11%2C+2012-AoH&utm_campaign=BNT+06112012&utm_medium=email.

[8] Jim Finkle & Jospeh Menn, *Part of "Flame" Code Found in Iranian Computers Same as Stuxnet*, Nat'l Post (June 11, 2012), *available at* http://news.nationalpost.com/2012/06/11/part-of-flame-code-found-in-iranian-computers-same-as-stuxnet/.

[9] *See, e.g.,* David P. Fidler, *Tinker, Tailor, Soldier, Duqu: Why Cyberespionage is More Dangerous Than You Think*, 5 (1) Int'l J. Critical Infrastructure Protection 28-29 (Mar. 2012).

[10] *See* Lance Whitney, *Flame Virus Could Attack Other Nations*, CNet.com (May 30, 2012), *available at* http://news.cnet.com/8301-1009_3-57443487-83/flame-virus-could-attack-other-nations/ (quoting ITU's cybersecurity coordinator).

[11] Hillary Clinton, U.S. Sec'y of State, Remarks at the Special Operations Command Gala Dinner (May 23, 2012), *available at* http://www.state.gov/secretary/rm/2012/05/190805.htm.

[12] *See, e.g., Hillary Clinton Boasts of US Cyberwar Against Al-Qaeda*, Telegraph (May 24, 2012), *available at* http://www.telegraph.co.uk/news/worldnews/al-qaeda/9286546/Hillary-Clinton-boasts-of-US-cyberwar-against-al-Qaeda.html.

[13] *See* Benjamin Wittes, *State Department Hackers?*, Lawfare Blog (May 24, 2012), *available at* http://www.lawfareblog.com/2012/05/state-department-hackers/.

[14] *See, e.g., Hacking Terrorist Websites Commonplace*, Investigative Project on Terrorism (June 3, 2011), *available at* http://www.investigativeproject.org/2937/hacking-terrorist-websites-commonplace*;* andAdam Rawnsley, *Stop the Presses! Spooks Hacked al-Qaide Online Mag*, Wired.com (June 1, 2011), *available at* http://www.wired.com/dangerroom/2011/06/stop-the-presses-spooks-hacked-al-qaida-online-mag/.

[15] Internet Society, *World IPv6 Launch* (June 6, 2012), *available at* http://www.internetsociety.org/deploy360/events/world-ipv6-launch/.

[16] Internet Engineering Task Force, *Internet Protocol, Version 6 (IPv6) Specification*, RFC 2460 (Dec. 1998).

[17] Stephen Shankland, *Internet Co-Creator Vint Cerf Welcomes IPv6 Elbow Room*, CNet.com (June 5, 2012), *available at* http://news.cnet.com/8301-1023_3-57447207-93/internet-co-creator-vint-cerf-welcomes-ipv6-elbow-room-q-a/.

[18] *Id.*

[19] *See, e.g.,* Kenneth Geers, *Strategic Cyber Defense: Which Way Forward?*, NATO Cooperative Cyber Defence Centre of Excellence (2012), *available at* http://www.ccdcoe.org/articles/2012/Geers_StrategicCyberDefense.pdf ("From a law enforcement and counterintelligence perspective, IPv6 could help to solve the problem of anonymous cyber attacks."); and White House, *National Strategy to Secure Cyberspace*, at 30 (Feb. 2003) (observing that IPv6 "provides for improved security features, including attribution and native IP security").

[20] *See, e.g.,* Dan Worth, *Move to IPv6 Could Lead to Huge Jump in Cyber Crime*, V3.co.uk (Sept. 8, 2011), *available at* http://www.v3.co.uk/v3-uk/news/2107731/ipv6-lead-huge-jump-cyber-crime (quoting official at the British Serious Organised Crime Agency arguing that IPv6 will make addressing cyber crime more complicated); and Geers, *supra* note 19, at 3 (noting that "human rights groups fear that governments will use this new capability to quash political dissent by reducing online anonymity and privacy").

[21] *See, e.g.,* Amy Schatz, *U.S. Firms Challenge Web-Oversight Proposals*, Wall Street J. (May 30, 2012), *available at* http://online.wsj.com/article/SB10001424052702304821304577436681230307676.html.

[22] International Telecommunications Union, International Telecommunication Regulations, Dec. 9, 1988 (Final Acts of the World Administrative Telegraph and Telephone Conference, WATTC-88), *available at* http://www.itu.int/osg/csd/wtpf/wtpf2009/documents/ITU_ITRs_88.pdf.

[23] Internet Society, World Conference on International Telecommunications [WCIT], *available at* http://internetsociety.org/wcit ("The decisions made by governments at WCIT could redefine the international regulatory environment for the Internet and telecoms in the 21st century and beyond—impacting how people around the world are able to use the Internet. Modifications to the ITRs could

result in changes to the Internet's architecture, operations, content and security.").

[24] *See, e.g.,* Wolfgang Kleinwachter, *The History of Internet Governance* (Oct. 2009), *available at* http://www.intgov.net/papers/35 (discussing the Internet governance controversy during the World Summit on the Information Society).

[25] *See, e.g.,* Simon Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law*, 27 Mich. J. Int'l L. 1071 (2006).

[26] *See* David P. Fidler, *Was Stuxnet an Act of War? Decoding a Cyberattack*," IEEE Security & Privacy, at 56-59 (July/Aug. 2011).

[27] Council of Europe, Convention on Cybercrime, Nov. 23, 2001, ETS Treaty Series No. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/html/185.htm.

[28] For an evaluation of the Convention, *see* Michael A. Vatis, *The Council of Europe Convention on Cybercrime*, *in* Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy 207-223 (2010).

[29] *See* Patrick Goodenough, *Internet Regulation Returns to the International Agenda*, CNSNews.com (May 29, 2012), *available at* http://cnsnews.com/news/article/internet-regulation-returns-international-agenda (quoting Russian Prime Minister (now President) Vladimir Putin).

[30] U.S. House of Representatives, *Concurrent Resolution Expressing the Sense of Congress Regarding Actions to Preserve and Advance the Multistakeholder Governance Model Under Which the Internet Has Thrived,* H. Con. Res. 127, 112th Cong., 2d sess., at 1 (May 30, 2012).

[31] Sally Shipman Wentworth, *International Proposals to Regulate the Internet* (May 31, 2012), *available at* http://internetsociety.org/international-proposals-regulate-internet#overlay-context=.

[32] Eric Pfanner, *Debunking Rumors of an Internet Takeover*, N.Y. Times (June 11, 2012), *available at* http://www.nytimes.com/2012/06/11/technology/debunking-rumors-of-an-internet-takeover.html?pagewanted=all.

[33] White House, *International Strategy to Secure Cyberspace: Prosperity, Security, and Openness in a Networked World*, at 11 (May 2011).