Cyber Warfare:
Law and Policy Proposals for U.S. and Global Governance

by Stuart S. Malawer

Cybersecurity is the newest and most unique national security issue of the twenty-first century. Cyber warfare uses computer technologies as defensive and offensive weapons in international relations.[1] Until now, there has been no national debate within the United States over the concept of cyber warfare; neither its meaning nor the international laws that govern this concept have been discussed at any length, and nor have the domestic rules regarding it.

The debate over cyber warfare is only now emerging in the United States, the United Kingdom, and the foreign policy dialogue between the U.S., the Russian Federation, and other nations. "[M]uch of the debate on policies related to cyber war is happening behind closed doors."[2] National and international understanding and strategy should be developed, and infrastructure must be implemented nationally and internationally.

It is important to explain cyber warfare between states in the context of domestic and international affairs from a legal-political perspective.[3] This article does not contain a discussion of the related issue of cyberattacks by criminal organizations, terrorists, or nonstate actors.[4]

Background

Recent events have given great significance to the use of cyberspace in conflict among nations and international relations generally.

In early July 2009, a wave of cyber attacks, presumably from North Korea, temporarily jammed South Korean and American government websites.[5] This came in the midst of North Korea's multiple and serial missile launches, general diplomatic tension over North Korea's nuclear program, and sanctions threatened by the U.S. and United Nations. This Korean episode followed quickly on the heels of the already well-known Russian Federation's cyber attacks against Estonia in 2007 and Georgia in 2008. Other examples include Israeli cyber attacks on Syria in 2007 and U.S. use of cyber weapons in Iraq.[6]

As a response to the increasing use of cyber attacks in international relations, in June 2009 U.S. Secretary of Defense Robert M. Gates created a new defense cyber command[7] and nominated the director of the National Security Agency to head it. Senate confirmation is pending.[8] In bilateral relations, the United States and Russia have been "locked in a fundamental dispute" over the growing concern over cyber attacks.[9] President Barack Obama addressed the issue of cybersecurity in a major speech on May 29, 2009, and proposed a cybersecurity czar.[10] He nominated Howard A. Schmidt, formerly of Microsoft Corporation, to serve in that position.[11] This speech was accompanied by the release of the administration's *Cyberspace Policy Review*. In December 2009, the United States entered into talks with the Russian Federation on cybersecurity and cyber warfare.[12]

Questions are raised by these recent events include:

- Would the federal government monitor private-sector networks, thus raising a slew of privacy concerns and further fueling debates that were first raised during the George W. Bush era about wiretapping without warrents?
- What would be the expanding role of the military in defensive, offensive, and preemptive cyber operations as the military and the intelligence agencies prepare for digital war?
- What are the rules of international law concerning cyber warfare when a country is attacked and when can it be used prior to an attack?

- Have traditional international law rules that govern armed attack failed to keep current with technology and digital warfare?

Within the last few months, various governmental and expert reports have been issued. They include:

- *Cyberspace Policy Review — Assuring a Trusted and Resilient Information and Communications Infrastructure* (White House, May 2009) [13]
- *Cyber Security Strategy of the United Kingdom — Safety, Security and Resilience in Cyber Space* (U.K. Cabinet Office, June 2009) [14]
- *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (National Academy of Sciences and National Research Council, 2009) [15]
- *Securing Cyberspace for the 44th Presidency — A Report of the Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency* (Center for Strategic and International Studies, December 2008).[16]

Highlights from Recent Reports

Cyberspace Policy Review — Assuring a Trusted and Resilient Information and Communications Infrastructure (White House, May 2009)

This report was released in conjunction with President Obama's extended news conference on May 29, 2009. It states that the federal government is not organized to address cyberspace. It acknowledges a need to conduct a national dialogue on cybersecurity and that national security should be balanced with the protection of privacy rights and civil liberties that are guaranteed by the Constitution and that form the bedrock of American democracy.

The federal government should cooperate with other nations and the private sector to solve cybersecurity problems: "Only by working with international partners can the United States best address these challenges"[17]. The report points out a host of issues that need to be resolved, such as defining acceptable legal norms for territorial jurisdiction, sovereign responsibility, and the use of force. Development of national and regional laws to govern prosecution of cybercrime, data preservation, and privacy presents significant challenges.

The report declares that "the Nation's approach to cybersecurity over the past 15 years has failed to keep pace with the threat"[18]. The report does not address cyber warfare. It does not offer policies, but it notes a need for enhanced international cooperation.

Cyber Security Strategy of the United Kingdom — Safety, Security and Resilience in Cyber Space (U.K. Cabinet Office, June 2009)

Shortly after the Obama administration released its report, the United Kingdom released a report on cybersecurity. Their reports say that both the United States and the United Kingdom "are increasingly concerned by what they deem to be one of the 21st century's biggest security risks: the threat of cyber attacks"[19]. The U.K. report, like the U.S. report, calls for more international coordination. The report also calls for the creation of a central office of cyber security.

One interesting quote puts the issue of cyber attacks in a clear historical perspective: "Just as in the 19th century we had to secure the seas for our national safety and prosperity, and in the 20th century we had to secure the air, in the 21st century we also have to secure our advantage in cyber space. This Strategy — our first national Strategy for cyber security — is an important step towards that goal"[20].

The report acknowledges the need to comply with core constitutional issues: "Our approach to national security is clearly grounded in a set of core values, including: human rights, the rule of law, legitimate and accountable government, justice, freedom, tolerance and opportunity for all"[21]. It further acknowledges that the national security challenges transcend international boundaries.

In discussing the proposed new office of cyber security, the report declares that it needs to "identify gaps in the existing doctrinal, policy, legal and regulatory frameworks (both domestic and international) and where necessary, take action to address them"[22]. Unfortunately, as in the U.S. report, these shortcomings and defects are not identified, let alone addressed.

Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities (National Academy of Sciences and National Research Council, 2009)

This report by the National Academy of Sciences approaches more directly the task of delineating the public policy and legal issues of cyber warfare, but it does not give adequate pro-

posals to confront it. It defines "cyber attack" as "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks"[23]. This is distinguished from intelligence-gathering activity.

The report reviews the scant public writing on cyber attack and cyber warfare that started in the mid-1990s. One of the earliest studies addressing the strategic implications was published by the RAND Corporation.[24] While this newest report does not provide an analysis of U.S. policy regarding cyber attacks, it includes general findings and recommendations.

The authors hoped that their report would stimulate a public discussion of cyber attack as an instrument of foreign policy at the nexus of technology, policy, ethics, and national security. They consider that cyber weapons are so different from any other weapons that a new legal regime is needed. The authors draw a historical analogy with the debate over and study of nuclear issues fifty years ago. The report acknowledges that the rise of nonstate actors raises new and novel concerns.

The authors consider that a legal analysis of cyber attacks should be based upon the concepts of use of force and armed attack as described in the U.N. Charter. The authors believe that the law governing the legality of going to war and the law defining warlike behavior also applies to cyber attacks. The report declares that "today's policy and legal framework for guiding and regulating the U.S. use of cyberattack is ill-informed, undeveloped, and highly uncertain"[25].

The report concludes that "the conceptual framework that underpins the U.N. Charter on the use of force and armed attack and today's law of armed conflict provides a reasonable starting point for an international legal regime to govern cyberattacks"[26]. The authors recommend that the U.S. government should find common ground with other nations regarding cyber attacks.

Securing Cyberspace for the 44th Presidency — A Report of the Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency (Center for Strategic and International Studies, December 2008)

This report served as the basis for much of President Obama's speech of May 29, 2009, and its accompanying report. The report concluded that cybersecurity is now a major national security problem, that emerging U.S. policy must respect privacy and civil liberties, and that a comprehensive national security strategy should be developed that incorporates domestic and international dimensions.[27] The report declares that there is a need to modernize authorities, and recommends that the White House should take the lead. "U.S. laws for cyberspace are decades old, written for the technologies of a less-connected era. Working with Congress, the next administration should update these laws."[28]

Major Issue Confronting the U.S. and Global System

The United States and other nations should create a sustainable global legal structure that promotes cooperation among nations to confront cyber warfare. Laws that govern the use of force and armed attacks under the U.N. Charter need to be clarified in this digital era. President Obama's reliance on a resurrected notion of the "just war doctrine," as enunciated in his acceptance speech for the Nobel Peace Prize in Oslo, further heightens the need for legal clarity.[29] Is the best defense against cyber attacks the use of robust offensive actions in cyberspace, and is it lawful?[30]

The Convention on Cybercrime adopted by the Council of Europe in 2001 is a good starting place, in addition to the U.N. Charter, in formulating a strategy to update the rules of law and to create a global governance structure to regulate cyber warfare.[31] The U.S. Senate ratified this convention in August 2006 and entered it into force in 2007. The convention highlights the many issues that play a role in regulating cybercrime. It defines five criminal offenses: illegal access, illegal interception, data interference, system interference, and misuse of devices. Even though the Russian Federation is not a member of the Convention on Cybercrime and argues that cross-border searches to investigate Internet crime violates its constitution,[32] the complex issue of regulating cyber warfare is addressed by this convention. National sovereignty, privacy and territorial integrity, and mutual assistance should be considered in formulating a new strategy for cyber warfare.

Proposal

Cyber warfare requires greater international legal and diplomatic initiatives — both bilateral and multilateral. Nations have a mutual interest in limiting any resort to cyber warfare.[33] A limitation could help prevent the destruction of both governmental and civil infrastructure and protect the welfare of millions of people. As early as July 2000, the Russian Federation submitted to the United Nations General Assembly a draft resolution, "Principles of International Information Security," that would prohibit the creation and use of tools for a cyber attack.[34]

A diplomatic conference should be convened similar to the naval and disarmament conferences in the interwar period.[35] Attendees could draft a global treaty to regulate cyber warfare and create political institutions that would enforce the adopted rules. The most important set of rules would limit the offensive use of cyber warfare in international relations.

In the interwar period of the 1920s and 1930s, naval conferences limited the number of capital ships (battleships) of the major powers that were capable of offensive operations.[36] The general disarmament conferences limited the right to go to war.[37] However, there were no limitations on the then newest form of offensive weapons — the aircraft carrier.[38] It would probably have been too late. Fleets of aircraft carriers were already afloat. These diplomatic conferences provided "hallow results" and "proved to be a monument to illusion."[39] Like those aircraft carriers that subsequently attacked Pearl Harbor, cyber warfare needs to be restricted and regulated.

The global community saw the consequences of the accumulated failure of the interwar conferences come to fruition in the late 1930s and, for the United States, on December 7, 1941.

This should be sufficient motivation to get it right this time, in the twenty-first century.

Endnotes:

1 General Wesley Clark recently wrote that "There is no form of military combat more irregular than an electronic attack. … It is tempting for policymakers to view cyberwarfare as an abstract future threat." Clark and Levin, "Securing the Information Highway: How to Enhance the United States Electronic Defenses." *Foreign Affairs* 2 (November / December 2009).

2 *Virtual Criminology Report 2009 — Virtually Here: The Age of Cyber Warfare.* 3 (McAfee 2009). This report, released late in 2009, discusses some of the broader and related issues of cyber warfare as well as the implications for the private sector and critical infrastructures.

3 This involves the use of such "weapons" as "logic bombs," "botnets," and microwave radiation that would be used to invade private, government, and military networks.

4 "FBI Suspects Terrorists Are Exploring Cyber Attacks." *Wall Street Journal* (November 18, 2009). Recent Chinese intrusions into Google servers highlight the foreign policy implications of state-sponsored computer intrusions for non-military reasons (commercial and censorship). This has set off a foreign-policy debate in the United States over global Internet freedom parallel to the emerging national-security debate over intelligence gathering and cyberwarfare. "Patriotism and Politics Drive China Cyberwar." *Financial Times* (January 14, 2010); "Web Access is New Clinton Doctrine." *Wall Street Journal* (January 21, 2010).

5 "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea." *New York Times* (July 9, 2009). This attack utilized roughly two hundred thousand computers that resulted in denial of services to both U.S. and Korean government and commercial websites. The attack utilized portions of the five-year-old MyDoom virus. Some experts consider this attack might have been by ordinary criminals. "Crippling Cyber-Attacks Relied on 200,000 Computers." *Financial Times* (July 10, 2009).

6 Only recently was it disclosed that militants in both Iraq and Afghanistan used off-the-shelf technology to intercept live feeds from U.S. Predator drones. "Officers Warned of Flaw in U.S. Drones in 2004." *Wall Street Journal* (December 12, 2009).

7 "Military Command Is Created for Cyber Security," *Wall Street Journal* (June 24, 2009).

8 "Beyond a cyber command, the Pentagon is grappling with a dizzying array of policy and doctrinal questions involving cyber warfare." "Questions Stall Pentagon Computer Defenses." *Washington Post* (January 3, 1010).

9 "U.S. and Russia Differ on a Treaty for Cyberspace," *New York Times* (June 28, 2009).

10 "Obama Outlines Coordinated Cyber-Security Plan," *New York Times* (May 30, 2009).

11 "Obama Names Howard Schmidt as Cybersecurity Coordinator." *Washington Post* (December 22, 2009).

12 This is a new American approach that differed from its earlier position that both the commercial and military use of software should be discussed together. "In Shift, U.S. Talks to Russia on Internet Security." *New York Times* (December 13, 2009). [Hereinafter cited as *U.S.-Russia Talks.*]

13 *Cyberspace Policy Review — Assuring a Trusted and Resilient Information and Communications Infrastructure* (White House, May 2009). [Hereinafter cited as *Obama Policy Review.]* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

14 *Cyber Security Strategy of the United Kingdom — Safety, Security and Resilience in Cyber Space* (U.K. Cabinet Office, June 2009). [Hereinafter cited as *U.K. Cyber Report*.] http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf

15 *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (National Academy of Sciences and National Research Council, 2009). [Hereinafter cited as *National Research Council Report.*] http://books.nap.edu/openbook.php?record_id=12651&page=R1

16 *Securing Cyberspace for the 44th Presidency — A Report of the Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency* (Center for Strategic and International Studies, December 2008). [Hereinafter cited as *CSIS Report.*] http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

17 *Obama Policy Review* iv.

18 *Id.* v.

19 "Cyber Security Risk," *Financial Times* (June 26, 2009).

20 *U.K. Cyber Report* 5.

21 *Id.* 10.

22 *Id.* 18.

23 *National Research Council Report* S-1.

24 *Strategic Information Warfare: A New Face of War* (Rand Corporation 1996) as cited in *National Research Council Report* viii. This report identifies the earlier writings from 1998 to 2009 discussing international law and digital warfare. *Id.* at note 5 at viii. *See also*, Dept. of Defense, Office of General Counsel, *Assessment of International Legal Issues in Information Operations*. (Dept. of Defense 1999).

25 *National Research Council Report* S3.

26 Id.

27 *CSIS Report* 1

28 *Id.* 2.

29 "Remarks by the President at the Acceptance of the Nobel Peace Prize" (December 10, 2009). http://www.whitehouse.gov/the-press-office/remarks-president-acceptance-nobel-peace-prize.

30 "U.S. Steps Up Effort on Digital Defenses." *New York Times* (April 28, 2009).

31 *Convention on Cybercrime* (concluded in Budapest on November 23, 2001).

32 *U.S.-Russia Talks.*

33 Countries such as China and North Korea may view cyber warfare as advantageous in an asymmetrical conflict with the United States.

34 Cited in *National Research Council Report* at 10-9.

35 "Genuine disarmament was never attempted after World War I, merely arms reduction and limits on certain types of naval weapons." *T. Bailey, A Diplomatic History of the American People* 654 (9th edition, 1974). [Hereinafter cited as *Bailey*.]

36 "The Five-Power Naval Treaty of Washington" (signed February 6, 1922); "The London Naval Conference" (signed April 22, 1930); "The Second London Naval Conference" (signed March 1936).

37 "The Pact of Paris" also known as "The Kellogg-Briand Pact." (signed August 27, 1928).

38 *Bailey* note 10 at 640.

39 *Id*. 648, 650.