



## **CYBERWARFARE**

### ***LAW AND POLICY PROPOSALS FOR U.S. AND GLOBAL GOVERNANCE***

**By Stuart S. Malawer, *J.D., Ph.D.***

*Distinguished Service Professor of Law & International Trade  
George Mason University\**

### **INTRODUCTION**

Cybersecurity is the newest and most unique national security issue of the 21st century. The most critical aspect of this issue is the notion of cyberwarfare, which is the use of computer technologies as both defensive and offensive weapons in international relations. Until now, there has been no national debate within the United States over the concept of cyberwarfare; neither its meaning nor the international laws governing this concept have been discussed at any length, to say nothing of the domestic rules regarding it.

The debate over cyberwarfare is only now emerging in the United States, the United Kingdom, and in the foreign policy dialogue between the United States, the Russian Federation, and other nations. National and international understanding and strategy need to be developed, and architecture must be implemented, both nationally and internationally.

In this paper, I address the concept of cyberwarfare in the context of both domestic and international affairs from a legal-political perspective. First, I examine recent government and private reports on cybersecurity and cyberwarfare. Second, I outline what I consider the major issue that confronts the United States and the global system as they struggle to address the

---

\* Stuart Malawer holds the *J.D.* from the Cornell Law School and the *Ph.D.* from the University of Pennsylvania (International Relations). He recently published the casebook *U.S. NATIONAL SECURITY LAW* (Wm. Hein & Co., 2009) with the *Introduction* by U.S. Senator Patrick Leahy, Chairman of the U.S. Senate Judiciary Committee. Dr. Malawer is the *Distinguished Professor of Law and International Trade* at the George Mason University (School of Public Policy). Paper submitted July 15, 2009.

dangers of cyberwarfare. Third, I conclude by proposing a method to begin structuring a comprehensive security strategy, taking into consideration the many domestic and global stakeholders.



## BACKGROUND

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

In early July 2009, a wave of cyberattacks, presumably from North Korea, temporarily jammed South Korean and American government websites.<sup>1</sup> This came in the midst of North Korea's multiple and serial missile launches, general diplomatic tension over North Korea's nuclear program, and threatened U.S. and U.N. sanctions. This Korean episode followed quickly upon the heels of the already well-known Russian Federation's cyberattacks against Estonia in 2007 and against Georgia in 2008.

As a response to the increasing use of cyberattacks in international relations, Defense Secretary Robert Gates in June 2009 created a new military command concerning cybersecurity.<sup>2</sup> He then recommended that the director of the National Security Agency assume the additional responsibility as commander of Cyber Command. In bilateral relations, the United States and Russia are "locked in a fundamental dispute" over the growing concern over cyberattacks.<sup>3</sup> The issue of the legal and political aspects of cyberattacks is expected to be raised by the Russian Federation in the U.N. General Assembly this fall. President Obama addressed the issue of cybersecurity in a major speech on May 29, 2009, and proposed a Cybersecurity Czar.<sup>4</sup> This speech was accompanied by the release of the administration's *Cyberspace Policy Review*.

---

<sup>1</sup> "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea," *New York Times* (July 9, 2009). This attack utilized roughly 200,000 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).

<sup>2</sup> "Military Command Is Created for Cyber Security," *Wall Street Journal* (June 24, 2009).

<sup>3</sup> "U.S. and Russia Differ on a Treaty for Cyberspace," *New York Times* (June 28, 2009).

<sup>4</sup> "Obama Outlines Coordinated Cyber-Security Plan," *New York Times* (May 30, 2009).

From the perspective of U.S. policy, many critical questions are raised by these recent events. Among others, they include:

- Would the federal government monitor private-sector networks, thus raising a slew of privacy concerns and further fueling debates on wiretapping without warrants that were first raised during the Bush era?
- What would be the expanding role of the military in defensive, offensive and preemptive cyberoperations as the military and the intelligence agencies gear up for digital war?
- Where would the new "Cyber Czar" be located in the White House or elsewhere?
- What are the rules of international law concerning cyberwarfare? For example, its use when attacked and when can it be used prior to an attack?
- Have traditional international law rules concerning 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, among others:

- *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure* (White House, May 2009)<sup>5</sup>
- *Cyber Security Strategy of the United Kingdom – Safety, Security and Resilience in Cyber Space* (U.K. Cabinet Office, June 2009)<sup>6</sup>
- *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (National Academy of Sciences and National Research Council, 2009)<sup>7</sup>
- *Securing Cyberspace for the 44<sup>th</sup> Presidency – A Report of the Center for Strategic and International Studies Commission on Cybersecurity for the 44<sup>th</sup> Presidency* (Center for Strategic and International Studies, December 2008).<sup>8</sup>

---

<sup>5</sup> 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](http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf)

<sup>6</sup> 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>

<sup>7</sup> 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](http://books.nap.edu/openbook.php?record_id=12651&page=R1)

<sup>8</sup> Securing Cyberspace for the 44<sup>th</sup> Presidency – A Report of the Center for Strategic and International Studies Commission on Cybersecurity for the 44<sup>th</sup> Presidency (Center for Strategic and International Studies, December 2008). [Hereinafter cited as CSIS Report.] [http://csis.org/files/media/isis/pubs/081208\\_securingcyberspace\\_44.pdf](http://csis.org/files/media/isis/pubs/081208_securingcyberspace_44.pdf)

## HIGHLIGHTS FROM RECENT REPORTS

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

This is the report that was released in conjunction with President Obama’s extended news conference on May 29, 2009. The report declares that the federal government is not organized to address the general issue of cyberspace. It acknowledges that there is a need to conduct a national dialogue on cybersecurity, and that there needs to be a balance between national security and the protection of privacy rights and civil liberties that are guaranteed by the Constitution and that constitute the bedrock of American democracy.

The United States government needs to cooperate with the private sector and other nations to solve cybersecurity problems: “Only by working with international partners can the United States best address these challenges ....”<sup>9</sup> The report points out a host of issues that need to be resolved, such as defining acceptable legal norms concerning territorial jurisdiction, sovereign responsibility, and the use of force. In addition, national and regional laws concerning prosecution of cybercrime, data preservation and privacy present 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.”<sup>10</sup> The report does not specifically deal with the issue of cyberwarfare. It does not offer any proposals concerning development of the rules of the game, but notes the 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)***

Amazingly, shortly after the Obama administration released its report, the United Kingdom released its report on cybersecurity. This almost joint release of reports evidences the fact that both the United States and the United Kingdom “are increasingly concerned by what they deem to be one of the 21<sup>st</sup> century’s biggest security risks: the threat of cyber attacks.”<sup>11</sup> 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 (OCS).

One interesting quote from the report puts the issue of cyberattacks in a clear historical perspective: “Just as in the 19<sup>th</sup> century we had to secure the seas for our national safety and prosperity, and in the 20<sup>th</sup> century we had to secure the air, in the 21<sup>st</sup> 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.”<sup>12</sup>

---

<sup>9</sup> Obama Policy Review iv.

<sup>10</sup> Id. v.

<sup>11</sup> “Cyber Security Risk,” Financial Times (June 26, 2009).

<sup>12</sup> U.K. Cyber Report 5.

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.”<sup>13</sup> 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 ....”<sup>14</sup> 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 cyberwarfare, but does not give adequate proposals to confront it. It defines “cyberattack” as “the 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.”<sup>15</sup> This is distinguished from intelligence-gathering activity.

The report reviews the scant public writing on cyberattack and cyberwarfare that started in the mid-1990s. One of the earliest studies addressing the strategic implications was published by the RAND Corporation.<sup>16</sup> While this newest report does not provide an analysis of U.S. policy regarding cyberattacks, it includes a number of general findings and recommendations.

The authors hoped that their report would stimulate a public debate on and discussion of cyberattack as an instrument of foreign policy at the nexus of technology, policy, ethics and national security. They consider cyberweapons so different from any other weapons that a new legal regime is needed. The authors draw an historical analogy with the debate and study of nuclear issues 50 years ago. The report acknowledges that, unlike 50 years ago, the rise of non-state actors raises new and novel concerns.

The authors consider that a legal analysis of cyberattacks should be based upon the concepts of “use of force” and “armed attack” as utilized in the U.N. Charter. In addition, the authors believe that the law governing the legality of going to war and the law defining warlike behavior also applies to cyberattacks. The report declares that “today’s policy and legal framework for

---

<sup>13</sup> Id. 10.

<sup>14</sup> Id. 18.

<sup>15</sup> National Research Council Report S-1.

<sup>16</sup> 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 1998-2009 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).

guiding and regulating the U.S. use of cyberattack is ill-informed, undeveloped, and highly uncertain."<sup>17</sup>

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."<sup>18</sup> The authors recommend that the U.S. government should find common ground with other nations regarding cyberattacks.

***Securing Cyberspace for the 44<sup>th</sup> Presidency – A Report of the Center for Strategic and International Studies Commission on Cybersecurity for the 44<sup>th</sup> 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's three major findings are: cybersecurity is now a major national security problem; emerging U.S. policy must respect privacy and civil liberties; and there is a need for a comprehensive national security strategy that incorporates domestic and international dimensions.<sup>19</sup> More specifically, the report notes 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."<sup>20</sup>

**MAJOR ISSUE CONFRONTING THE U.S. AND GLOBAL SYSTEMS**

The major issue, in my opinion, that confronts the United States and other nations is the need to create a sustainable global legal structure that promotes cooperation among nations to confront cyberattacks and, more specifically, cyberwarfare. It is clear to me that the traditional legal structure governing the use of force and armed attacks under the U.N. Charter needs to be greatly clarified in this digital era. For the United States, a major policy issue confronting it is whether if the best defense against cyberattacks is the use of robust offensive actions in cyberspace.<sup>21</sup>

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 regulating cyberwarfare.<sup>22</sup> The U.S. Senate ratified this convention in August 2006. The convention highlights the many issues that play a role in regulating cybercrime. It defines five criminal offenses specifically: illegal access; illegal interception; data interference; system interference; misuse of devices. The much more serious issue of regulating cyberwarfare can be approached from the advantage of the debate and experience under this convention. Traditional issues, as already mentioned in the various

---

<sup>17</sup> National Research Council Report S3.

<sup>18</sup> Id.

<sup>19</sup> CSIS Report 1.

<sup>20</sup> Id. 2.

<sup>21</sup> "U.S. Steps Up Effort on Digital Defenses." New York Times (April 28, 2009).

<sup>22</sup> Convention on Cybercrime (concluded in Budapest on November 23, 2001).

reports, of national sovereignty, privacy and territorial integrity, and mutual assistance are ones that need to be considered in formulating a new strategy for cyberwarfare.

## PROPOSAL

Cyberwarfare is already upon us and new international legal and diplomatic initiatives are required, both bilateral and multilateral. The major players in the global system today have a mutual interest in limiting resort to cyberwarfare.<sup>23</sup> This could help prevent the destruction of both governmental and civil infrastructure and ensure the welfare of millions of people. It is interesting to note that in July 2000 the Russian Federation submitted to the General Assembly a draft resolution, "Principles of International Information Security" that would prohibit the creation and use of tools for a cyberattack.<sup>24</sup>

A diplomatic conference similar to the naval and disarmament conferences in the interwar period should be called.<sup>25</sup> Attendees could draft a global treaty regulating cyberwarfare and create political institutions that would enforce the adopted rules. The most important set of rules would provide a genuine limit to the offensive use of cyberwarfare in international relations.

In the interwar period of the 1920s and 1930s the naval conferences limited the number of capital ships (battleships) of the major powers that were capable of offensive operations.<sup>26</sup> The general disarmament conferences limited the right to go to war.<sup>27</sup> However, there were no limitations whatsoever placed on the then newest form of offensive weapons, the aircraft carrier.<sup>28</sup> 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."<sup>29</sup> Like those aircraft carriers that subsequently attacked Pearl Harbor cyberwarfare today 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 21<sup>st</sup> century.



---

<sup>23</sup> Countries such as China and North Korea may view cyberwarfare as advantageous in an asymmetrical conflict with the United States.

<sup>24</sup> Cited in National Research Council Report at 10-9.

<sup>25</sup> "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 (9<sup>th</sup> edition, 1974). [Hereinafter cited as Bailey.]

<sup>26</sup> "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).

<sup>27</sup> "The Pact of Paris" also known as "The Kellogg-Briand Pact." (signed August 27, 1928).

<sup>28</sup> Bailey note 10 at 640.

<sup>29</sup> Id. 648, 650.

## President Obama’s News Conference & Video on Cyberspace

(May 29, 2009)

### Seven Broad Points

1. Transformational moment.
2. “Weapons of Mass Disruption.”
3. New comprehensive approach.
4. To secure the “digital infrastructure.”
5. This is a “national security priority.”
6. Will not monitor private networks or Internet traffic. (“Network Neutrality”)  
-- Preserve and protect personal and private liberties that we cherish.
7. New office in White House – “Cybersecurity Coordinator.”

*“Information Age is only in its infancy – new world waits.”*

### Six Specific Items

- 1) Defense and military networks are under constant attack.
- 2) “Face of War” – Russian cyber attacks on Georgia (2008).
- 3) National security challenge.
- 4) Federal agencies have overlapping missions.
- 5) National Security Council (NSC) and Homeland Security Council (HSC) have done a top-to-bottom review.
- 6) Increase “private – public partnership.”

Note – President Obama did not address – Use of cyber tools in military conflict in case of attack or offensive use.

