THE CASE AGAINST AN INTERNATIONAL CYBERWARFARE CONVENTION

Lawrence L. Muir, Jr.[*]

INTRODUCTION

Over the past five years, a number of academic articles have called for the creation of an international convention to govern the rules, rights, and responsibilities of nations in cyber warfare and information operations.[1] Although cyber warfare by its nature is an international issue, the articles fail to recognize the overwhelming obstacles that will prevent a timely and meaningful agreement from taking form and why an agreement may not benefit the United States. This Essay addresses the need for clarification of cyber warfare laws from the perspective of strengthening the United States and protecting American citizens, businesses, and government.

The development of a legal regime around cyber warfare should have four goals: first, to protect the full panoply of property rights, second to minimize cyber attacks and reduce their collateral damage, third to deter the use of proxies in the commission of cyber attacks, and fourth to provide legal recourse for aggrieved parties. These goals are more likely to be realized if the United States unilaterally develops its own framework for cyber war.

This Essay will first briefly address the significant unresolved issues in cyber warfare. By laying out these issues, the Essay will suggest why an international framework will not be forthcoming, let alone effective. Next, the Essay will suggest a skeleton plan of how the United States can take the world lead in cyber war to protect its own interests and promote responsible behavior by other nations.

---

* Assistant Attorney General, Computer Crime Section, Office of the Attorney General of Virginia. He is a member of the Virginia Governor's Homeland Security Working Group. Beginning in January 2012, he will be an adjunct professor of law in cyber crime at Washington & Lee University School of Law. He thanks Lara Dresser of the Richmond Public Library for her research assistance, and his colleagues and father for their thoughtful commentary on the paper.

1. *See, e.g.*, Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023 (2007); Arie J. Schaap, *Cyberwarfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121 (2009); Scott J. Shackleford and Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971 (2011).

I. AN INTERNATIONAL FRAMEWORK IS UNLIKELY AND NOT ADVANTAGEOUS TO THE UNITED STATES

There is a general consensus that cyber attacks, whether for the purposes of crime, terrorism, or warfare, may have catastrophic effects. Moreover, there is a consensus that something must soon be done to protect the nation from cyber attacks. The problem is that when one looks behind these generic platitudes, the unresolved issues are so daunting that it is hard to know how to begin developing the framework, let alone how it should take form. The following paragraphs contain a brief overview of the ambiguities that will prevent any meaningful international discourse and resolution from taking place.

A. How to Classify Assets?

Attorneys seek to develop new laws through analogizing new actions to existing bodies of law. The nature of cyber attacks presents unique challenges to those analogies. Computer malware may be used to attack many different types of assets. Attacks may disable networks and websites,[2] shut down nuclear power plants,[3] or steal intellectual property.[4] A computer virus that shuts down a power grid in the United States can arguably be a crime because it intrudes upon the property of a business and causes it injury.[5] If that same power grid powers a military installation, it could be construed as an act against the military, possibly violating the Law of Armed Conflict ("LOAC").[6] Conversely, if Chinese cyber thieves stole the Google search algorithm,[7] that likely would not be a violation of international law.[8] That analysis may change if those

---

2. Hollis, *supra* note 1 at 1024–25 (reviewing the cyber attacks on Estonian networks and websites).

3. For more information about the Stuxnet virus, see Michael Joseph Gross, *A Declaration of Cyber-War*, VANITY FAIR, Apr. 2011, *available at* http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104.

4. For more information on Chinese cyber attacks on American private businesses during Operations Aurora and Shady RAT, see Michael Joseph Gross, *Enter the Cyber-Dragon*, VANITY FAIR, Sept. 2011, http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109.

5. See VA. CODE ANN. §18.2-152.4 (2010) as an example of a criminal law.

6. The Law of Armed Conflict is not codified. Rather it is the aggregation of international treaties and customs of international conduct by governments.

7. Google is a private business and its proprietary algorithm is private property owned by Google. The Google source code was the subject of what is now known Operation Aurora. Kim Zetter, *Google Hack Was Ultra Sophisticated, New Details Show*, WIRED.COM, THREAT LEVEL (Jan. 14, 2010 8:01 PM), http://www.wired.com/threatlevel/2010/01/operation-aurora/.

8. *See* Jack Goldsmith, *General Cartwright on Offensive Cyberweapons and Deterrence*, LAWFARE (Nov. 8, 2011 10:27 AM), http://www.lawfareblog.com/2011/11/general-cartwright-on-offensive-cyber-weapons-and-deterrence/.

same Chinese programmers stole Lockheed Martin's engineering research to gain the ability to sabotage a new American fighter jet.[9]

These hypothetical situations demonstrate the difficulties in selecting a body of law to apply to an international convention. Framers cannot make absolute judgments declaring attacks on certain asset classes, or targets, as crimes or acts of war because of the variables within the equation.[10] In addition, the consequences for treating attacks as a violation of the LOAC are so severe compared to violations of criminal law that an impasse in selecting the appropriate choice of laws could derail the entire negotiation. Countries that rely on cyber attacks primarily to commit crimes and espionage will seek to avoid LOAC classification, while countries with strong cyber warfare capabilities and significant cyber vulnerabilities will wish to reserve the ability to address cyber attacks with a military response.

B. Asymmetries in Cyber Warfare

The most significant impediment to an international resolution is the asymmetrical positioning of individual nations. The United States has considerable capabilities in cyber weapons,[11] but is also highly vulnerable to cyber attack due to the amount of information and dependence on computer networks. The technologies that put the United States in a position of strength may also be its Achilles' heel.

Compare the position of the United States to North Korea and China. If North Korea, which possesses cyber warfare capabilities,[12] shut down an American power grid, it would be

---

9. *See* Siobahn Gorman and Julian E. Barnes, *Cyber Combat: Act of War*, WALL ST. J., (May 31, 2011), http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html. Lockheed Martin is a private business, but here the stolen property would be both civilian and militarily owned. The property would also belong to the Department of Defense and the theft of the property is a threat against the U.S. military.

10. These variables include whether the target is a private or public entity, military or civilian, the type of information compromised, that information's national security value, and the direct and collateral damage done by the attack.

11. Damien McElroy, *Military Balance Report: Countries Creating New Cyber Warfare Organizations*, DAILY TELEGRAPH, Mar. 9, 2011, http://www.telegraph.co.uk/news/uknews/defence/8369520/Military-Balance-report-countries-creating-new-cyber-warfare-organisations.html. The United States has the preeminent cyber warfare capabilities, followed by Russia and China.

12. *See* Chico Harlan and Ellen Nakashima, *Suspected North Korean Cyberattack on Bank Raises Fears for S. Korea, Allies*, WASH. POST (Aug. 30, 2011), http://www.washingtonpost.com/world/national-security/suspected-north-korean-cyber-attack-on-a-bank-raises-fears-for-s-korea-allies/2011/08/07/gIQAvWwIoJ_story.html (detailing a North Korean cyber attack on Nonghyup agricultural bank in South Korea, causing their customers to be unable to access their accounts).

devastating. If the United States did the same to North Korea, would many North Koreans even notice? North Korea would never seek to subscribe to an international treaty curtailing cyber weapons knowing that it would be signing away a tool that cannot similarly be effectively deployed against it.

Likewise, the gains made by China by committing cyber attacks greatly outweigh China's vulnerabilities. China has been able to steal significant amounts of American intellectual property[13] that has jump started its economy at a fraction of the development cost.[14] Moreover, the People's Liberation Army has cyber warfare capabilities that enhance China's military capabilities.[15] The asymmetrical position of the United States as victim to China's theft makes it unlikely that China would sign any meaningful cyber security treaty. Moreover, China owns 9.8% of American debt,[16] further weakening the United States's negotiating position.[17] Finally, China's veto on the U.N. Security Council allows it to block any international treaty that contains meaningful protections against China's cyber units.

The nations that perpetrate cyber attacks against the United States have little incentive to negotiate limitations on cyber activities. If the United States understands the threat cyber economic espionage poses to its economic growth, it will have to take unilateral action to incentivize these states to eventually join an international convention.

---

13. *See* Gross, *supra* note 4.

14. Siobhan Gorman, *China Singled Out for Cyber Spying*, WALL ST. J. (Nov. 4, 2011), http://online.wsj.com/article/SB10001424052970203716204577015540198801540.html.

15. Kathrin Hille, *Chinese Military Mobilises Cybermilitias*, FINANCIAL TIMES (Oct. 12, 2011), http://www.ft.com/cms/s/0/33dc83e4-c800-11e0-9501-00144feabdc0.html#axzz1dAgZ8HRd (detailing the significant efforts made by the PLA to gain intelligence and do other activities against the West).

16. Peter Grier, *National Debt: Whom Does the United States Owe?*, CHRISTIAN SCI. MONITOR (Feb. 14, 2011), http://www.csmonitor.com/USA/Politics/DC-Decoder/2011/0204/National-debt-Whom-does-the-US-owe.

17. Admiral Mike Mullen stated over the summer of 2010 that the national debt was the biggest threat facing the United States in the future. *Mullen: Debt is Top National Security Threat*, CNN (Aug. 27, 2010), http://articles.cnn.com/2010-08-27/us/debt.security.mullen_1_pentagon-budget-national-debt-michael-mullen?_s=PM:US. Compare that to then CIA Director, now Secretary of Defense Leon Panetta's comment the Senate Armed Services Committee in June 2011 that, "The next Pearl Harbor we confront could very well be a cyber-attack that cripples our power systems, our grid, our security systems, our financial systems, our governmental systems." Laura Crimaldi, *Nations Fight Against Cyber Intruders Goes Local*, MSNBC.COM (July 20, 2011), http://www.msnbc.msn.com/id/43828271/ns/technology_and_science-security/t/nations-fight-against-cyber-intruders-goes-local/. It seems the debt and cyber security are not mutually exclusive, and that one threat may play into another.

C. The Difficulty of Attribution and Adopting a Correlative Legal Standard

Attribution is the ability to identify who attacked a computer network and from what location. This is a technological challenge because attackers have abilities to disguise their identities. The Stuxnet virus that obstructed Iranian nuclear ambitions at the Bushehr and Natanz plants has been studied by a number of international computer security experts. None have been able to definitively pinpoint the nation responsible for the attack or even identify the target.[18]

Attributing individual or group responsibility for attacks is even more difficult than national attribution. Cyber attackers fall into one of three categories. First, citizen hackers—individuals or small groups of hackers that band together for a common enterprise, whether for political motivation[19] or criminal enterprise.[20] Second, cyber militias—they have structural similarity to citizen hacking groups but are banded together by the state and may be given direction by state actors.[21] A cyber militia is a convenient partnership for a rogue state because its existence enables the nation to achieve state ends, but offers plausible deniability to the state.[22] Third, official state agencies—such as the 67th Network Warfare Wing of the United States Air Force.[23]

Attribution is an imperfect science, and as such leads to disagreement in selecting an applicable legal standard for determining the responsibility of states when either of the first two classes launches a cyber attack. Three legal standards have been

---

18. See Yossi Melman, *Iran Nuclear Worm Targeted Natanz, Bushehr Nuclear Sites*, HAARETZ.COM (Nov. 20, 2010), http://www.haaretz.com/news/diplomacy-defense/iran-nuclear-worm-targeted-natanz-bushehr-nuclear-sites-1.325596; *see also* Gross, *supra* note 3.

19. This is frequently referred to as hacktivism, and the group primarily responsible for this form of cyber warfare is known as "Anonymous." *See, e.g.*, Hannah Roberts, *Cashing in as the Face of Anonymous: Hacking Group Spokesman Lands a Six Figure Book Deal*, DAILY MAIL (Nov. 5, 2011 11:40 AM), http://www.dailymail.co.uk/news/article-2057884/Anonymous-spokesman-Barrett-Brown-lands-figure-book-deal.html?ito=feeds-newsxml.

20. *See* Hemanshu Nigam, *Mobsters, Taunters and More: The Four Kinds of Hackers*, ABC NEWS (July 19, 2011), http://abcnews.go.com/Technology/We_Find_Them/kinds-hackers-mobsters-taunters/story?id=13979327. These hackers are referred to as "mobsters" because they are linked with a new form of organized crime.

21. *See* Hille, *supra* note 15.

22. *See* Hollis, *supra* note 1 at 1025–28, for an explanation of the Russian cyber attacks against the Estonian government in the wake of a political dispute.

23. The United States Department of Defense has organized cyber units from all of the branches of the military under the United States Cyber Command, or "USCYBERCOM" at Fort Meade, home of the National Security Agency.

offered, each of which incentivizes states to use non-state actors to the detriment of protecting potential victims from cyber attacks.

As Shackelford and Andres have stated, the standards hinge on two separate issues: level of state control and prosecutorial burden of proof. As to the level of state control, the legal standard set forth by the International Court of Justice ("ICJ") in *Nicaragua*[24] holds that a state is liable for the actions of "paramilitaries or non-State actors only if the actors in question act in 'complete dependence' on the state."[25] The opposing "overall control" standard set forth in *Prosecutor v. Tadic*[26] holds that "where a State has a role in organizing, coordinating, and providing support for a group, the group's acts are attributable to the State.[27]

International law also differs on burden of proof. The ICJ relied on the *Nicaragua* effective control standard to decide Serbia's culpability in the genocide of Bosnian Muslims, but held that Serbia's guilt must be proven beyond any doubt, rather than beyond a reasonable doubt.[28] Due to the inherent difficulties in attribution, any international framework using the effective control standard for cyber attacks would be effectively neutered before it would ever be tested.

The differing international standards further demonstrate why the United States should not rely on an international framework. By agreeing to a framework using these standards, the United States would render itself vulnerable to uncontrolled rogue actors not accountable to any set of laws. These rogue actors may cause significant damage to the civilian population, but the heightened standard may enable the actors to escape responsibility, thereby encouraging damaging attacks. An international framework, therefore, may not be strong enough to protect American interests even if the framers and signatories are somehow able to agree on a standard to use.

II. THE UNITED STATES SHOULD CREATE ITS OWN FRAMEWORK

The United States probably has the highest level of vulnerability to a cyber attack based on its reliance on technology. That vulnerability, however, does not leave the U.S. in a weak negotiating position because it also possesses the strongest

---

24. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 110 (Jun. 27) (laying out the effective control standard); Shackelford and Andres, *supra* note 1 at 986.

25. *See* Shackleford and Andres, *supra* note 1 at 986.

26. *See* Prosecutor v. Tadic, Case No. IT-94-1-I, Decision on Defense Motion for Interlocutory Appeal on Jurisdiction (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995); Shackleford and Andres, *supra* note 1 at 986.

27. *See* Shackleford and Andres, *supra* note 1 at 986, for an explanation of the operational control standard.

28. *Id.*

cyber warfare capabilities.[29] Therefore, as both the strongest and most vulnerable nation, the United States is most in need of establishing the laws and consequences regarding foreign cyber attacks.

The outline of this American framework would address the aforementioned issues in this way. First, the United States should create a protected class of cyber assets and declare that an attack on any of the listed assets could trigger a military response from the United States. Those assets should include any military network, no matter the size or function. The list should protect the power grids, air traffic control networks, and other assets that are used for both military and civilian functions and that are instrumental in the public safety of Americans. Protecting these assets is imperative to the welfare of the United States, the safety of its citizens, and the functioning of its economy.

One of the surprising issues revealed during the investigation into the attacks on Google was that Google believed the U.S. government would offer it some protection from foreign cyber attack.[30] To address this confusion, the U.S. government should build public-private partnerships with certain American businesses and offer to provide some measure of protection and support if attacked in exchange for the business sharing threat information and implementing cyber security enhancements. These public-private partnerships should include any business that falls into one of two categories: businesses that hold information for the U.S. government,[31] or those whose cyber security is vital to national security. The latter category will include technology companies, such as Google, whose technology is imperative to American technological and economic advantage, financial institutions who serve as repositories for the wealth of the nation, and other appropriate industries. If a nation attacks a business in one of those categories, the United States would reserve the right to respond with its military or law enforcement personnel.

The LOAC promotes the necessity of organized warfare fought through official state action, and cyber warfare should be no different. The American framework should remove the distinction between state and non-state actors where culpability is at issue. If the United States can present *prima facie* evidence that a foreign

---

29. *See* Damien McElroy, *Military Balance Report: Countries Creating New Cyber Warfare Organizations*, THE TELEGRAPH (Mar. 9, 2011), http://www.telegraph.co.uk/news/uknews/defence/8369520/Military-Balance-report-countries-creating-new-cyber-warfare-organisations.html.

30. *See* Gross, *supra* note 4 (explaining that Google told the NSA after its source code had been attacked that Google thought the NSA protected them from actions of that nature).

31. For example, defense contractors hold significant amounts of military research, and therefore their networks should have to comply with Department of Defense standards.

nation had any knowledge of the actions of individual hackers or a cyber militia group in an attack on U.S. assets, the United States should reserve the right to make an equivocal response and seek legal recourse. The equivocal response is the big stick the United States possesses to protect its assets, while the legal recourse promotes its willingness to settle matters peacefully rather than militarily when appropriate.[32] By incentivizing states to control their hackers and cyber militias, the United States will promote compliance with international law and minimize collateral damage from cyber attacks. This policy will have the effect of promoting caution in using cyber attacks and raising the treatment of cyber warfare to be on par with traditional warfare.

CONCLUSION

A significant number of challenges await the treaty negotiators that will draft the international framework for cyber warfare. Those challenges, ultimately, will thwart the promulgation of a timely and meaningful treaty. In the meantime, the United States government, American businesses, and American citizens will continue to be victimized by foreign cyber attacks at great loss to our financial and intellectual capital. It is time for the United States to unilaterally set its standards to maximize the protection of the aforementioned groups. The United States must act soon, not just to reduce the outflow of this capital, but also because it is still the preeminent cyber warfare power. Not acting will jeopardize that standing, and if that happens, the nation's economic strength will be at the mercy of foreigners sitting behind computer screens.

32. Legal recourse options may include suits against foreign nations, prosecution of suspected perpetrators, but may also include policy decisions such as the suspension of foreign aid to the nations allowing the actors to function.