12-2011

The Case Against an International Cyber Warfare Convention

Lawrence L. Muir Jr.
Washington and Lee University School of Law, muirl@wlu.edu

I. 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 the United States may not benefit from one. This paper 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 these goals: protect the full panoply of property rights, minimize cyber attacks and reduce their collateral damage, deter the use of proxies in the commission of cyber attacks, and provide legal recourse for aggrieved parties. These goals are more likely to be realized, and sooner, if the United States unilaterally develops its own framework independent of other nations.

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

---

[1] For example, see Hollis, Duncan B. "Why States Need an International Law for Information Operations," Lewis & Clark Law Review, Winter 2007, Symposium Crimes, War Crimes, and the War on Terror. See also Major Arie J. Schapp, "Cyber Wafare Operations: Development and Use under International Law," Air Force Law Review Cyberlaw Edition (2009). See also Shackleford, Scott J. and Richard B. Andres. "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem." Georgetown Journal of International Law, Summer 2011, 2011 Symposium on International Cyberlaw.

II. Legal and factual ambiguities will impede an international framework and may leave the United States more vulnerable to cyber attack.

There is a general consensus that cyber attacks, whether for the purposes of crime, terrorism, or warfare, can have catastrophic effects. Moreover, there is a consensus that something must be done, and soon. 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. The different types of assets that may be attacked causes difficulty in selecting a body of law to use as a base for the international framework.

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

[2] Hollis, Duncan B. Why States Need an International Law for Information Operations. Lewis & Clark Law Review, Winter 2007. Symposium on Crimes, War Crimes, and the War on Terror.
[3] For more information about the Stuxnet virus, see Gross, Michael Joseph, "A Declaration of Cyber-War," Vanity Fair, April 2011.
[4] For more information on Chinese cyber attacks on American private businesses during Operations Aurora and Shady RAT, see Gross, Michael Joseph, "Enter the Cyber-dragon," Vanity Fair, September 2011.
[5] See §18.2-152.6 of the *Code of Virginia* as an example of a criminal law.

act against the military, possibly violating the Law of Armed Conflict (LOAC).[6] If Chinese cyber thieves stole the Google search algorithm,[7] would that be a crime or a violation of the LOAC? Would the analysis change if those same Chinese programmers stole Lockheed Martin's engineering research for a new American fighter jet?[8]

These four hypothetical situations demonstrate the difficulties in selecting a body of law to apply to cyber attacks. 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.[9] 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 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 of national cyber vulnerabilities and capabilities discourage an international framework.

The most significant impediment to an international resolution is the asymmetrical positioning of individual nations. The United States has considerable

---

[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.

[8] See Gorman, Siobahn and Julian E. Barnes, "Cyber Combat: Act of War," Wall Street Journal, May 31, 2011. Lockheed Martin is a private business, but here the stolen property would be both civilian and militarily owned.

[9] 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.

capabilities in cyber weapons,[10] but is also highly vulnerable to cyber attack due to the amount of information and dependence on computer networks. The technologies that make the United States so strong 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,[11] would shut down an American power grid, it would cause devastating damage to many facets of American life. 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 in its terror arsenal that cannot similarly be deployed against it to much effect.

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[12] that has jump started its economy at a fraction of the cost to honestly develop that technology.[13] Moreover, the People's Liberation Army has cyber warfare capabilities that have enhanced China's military capabilities.[14] The asymmetrical position of the United States as victim to China as thief makes it unlikely that China would sign any meaningful cyber security treaties. Moreover, China owns 9.8% of

[10] McElroy, Damien. "Military Balance report: countries creating new cyber warfare organisations." March 9, 2011. Daily Telegraph (UK). The United States has the preeminent cyber warfare capabilities, followed by Russia and China.
[11] See Harlan, Chico and Ellen Nakashima. "Suspected North Korean Cyberattack on Bank raises fears for S. Korea, allies." Washington Post, August 30, 2011. This article details a North Korean cyber attack on Nonghyup agricultural bank in South Korea, causing their customers to be unable to access their accounts.
[12] See Gross, "Enter the Cyber-Dragon."
[13] Gorman, Siobhan. "China Singled Out for Cyber Spying." Wall Street Journal, Friday, November 4, 2011.
[14] Hille, Kathrin. "Chinese military mobilises cybermilitias." Financial Times, October 12, 2011, detailing the significant efforts made by the PLA to gain intelligence and do other activities against the West.

American debt,[15] further weakening the United States's negotiating position.[16] Finally, China's veto on the United Nations Security Council allows it to block any international treaty that contains meaningful protections to the cyber vulnerable nations against China's cyber units.

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

C. The difficulty of attribution and choice of legal standards encourages rogue cyber attack groups.

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.[17] None have been able to even conclusively identify the target.[18]

---

[15] Grier, Peter. "National Debt: Whom Does the United States Owe?" Christian Science Monitor, February 14, 2011.

[16] Admiral Mike Mullen stated repeatedly over the summer of 2010, including to CNN on August 26, 2010, that the national debt was the biggest threat facing the United States in the future. 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 could very well be a cyber-attack that cripples our government, security and financial system." It seems the debt and cyber security are not mutually exclusive, and that one threat may play into another.

[17] See Melman, Yossi, "Iran nuclear worm targeted Natanz, Bushehr nuclear sites," November 20, 2010 on Haaretz.com. Compare to Gross, "A Declaration of Cyber-War."

[18] Id.

Attributing individual or group responsibility for attacks is even more difficult than national attribution. Cyber attackers fall into one of three categories. Citizen hackers are individuals or small groups of hackers that band together for a common enterprise, whether for political motivation[19] or criminal enterprise.[20] Cyber militias 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 their existence enables the nation to achieve state ends, but offers plausible deniability to the state.[22] The third classification is the official state agency classification, 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 offered, each of which incentivizes states to use non-state actors to the detriment of protecting potential victims from cyber attacks.

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 in the International Court of Justice *Nicaragua* case[24] holds that a state is liable for the

[19] This is frequently referred to as hacktivism, and the group primarily responsible for this form of cyber warfare is known as "Anonymous."
[20] See Nigam, Hemanshu, "Mobsters, Taunters and More: The Four Kinds of Hackers," on abc.com July 19, 2011. These hackers are referred to as "mobsters" because they are linked with a new form of organized crime.
[21] See Hille, "China mobilises cybermilitias."
[22] See Hollis, Duncan B. "Why States Need an International Law for Information Operations." 11 LCLR 1023, 1025-1028, 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.
[24] See Military and Paramilitary Activities in and against Nicaragua (Nicar. V. U.S.), 1986 I.C.J. 14 110 (Jun. 27) [hereinafter "Nicaragua"], laying out the effective control standard.

actions of paramilitaries or non-state actors only if the actors in question act in complete dependence on the state.[25] The opposing standard set forth in *Prosecutor v. Tadic*[26] case holds that, where a state has a role in organizing, coordinating, and supporting the group, the group's acts are attributable to the state.[27]

International law also splits on burden of proof. The International Court of Justice relied on the *Nicaragua* effective control standard of state involvement 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 this legal standard for cyber attacks would be effectively neutered before it would ever be tested.

The choice of international standards further demonstrates 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.

III. The United States should create its own framework with appropriate legal standards and defined responses to encourage foreign compliance.

---

[25] See Shackleford and Andres, "State Responsibility for Cyber Attacks," 42 GEOJIL 971, 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 Interlocutory Appeal on Jurisdiction. (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995) [hereinafter "Tadic"].
[27] See Shackleford, 986, explaining the operational control standard.
[28] Id.

The United States probably has the highest level of vulnerability to a cyber attack based on its reliance on technology. That vulnerability does not leave the U.S. in a weak negotiating position because it also possesses the strongest 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 United States 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 from attacks, and support if attacked, in exchange for the business sharing information and implementing cyber security enhancements. This classification should include any business that falls into one of two categories: businesses

[29] See, McElroy, Damien, "Military Report."
[30] See Gross, "Enter the Cyber-dragon," 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.

that hold information for the United States 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 vital 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 member of that list, 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 absolve 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 nation had any knowledge of the actions of individual hackers or a cyber militia group, the United States should reserve the right to make an equivocal response and seek legal recourse using this standard. 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 the international laws, and the collateral damage of cyber attacks should be minimized. This will have the effect of promoting caution in using cyber attacks and raise the treatment of cyber warfare to be on par with traditional warfare.

IV. Conclusion

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

[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.

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 in order 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.