Eleanor Mount

Jessica Beyer

JSIS B 355, Spring 2017

4 June 2017

Cyber Weapons and International Management

Introduction

In January 2010, inspectors with the International Atomic Energy Agency noticed centrifuges at the Natanz Uranium Enrichment Facility in Iran were failing at an unprecedented rate (Zetter). Soon after, inspectors discovered the equipment failure was caused by malware, or malicious software, that aimed to slow down the Iranian nuclear effort without overt military action. The malware, now known as Stuxnet, was created as part of a joint operation between the United States and Israel, though neither country has admitted to it (Thomson). Stuxnet is now known as the first cyber weapon that escaped the digital realm to cause physical damage to critical infrastructure across international boundaries (Lindsay).

This paper provides an overview of cyber weapons and the unique policy issues associated with governing their use. Part one defines cyber weapons as computer code that can cause physical harm. Part two identifies the policy problem as a lack of international consensus around cyber weapons, creating a realm for states to act without consequences. An examination of current policies in place regulating cyber weapons and how states may react to various policy proposals depending on their views of international law follows. In the final section, a solution is proposed around creating international agreements defining cyber weapons. Developing universal definitions and rules of conduct regarding cyber weapons will remain an urgent matters, as it is an area of policy that poses a significant threat to global safety but lacks preventative mechanisms.

The Cybersecurity Issue

Before delving into the policy problems surrounding cyber weapons in the international sphere, it is important to understand what cyber weapons are and why they create unique policy problems. Although the term “cyber weapon” is used commonly, it is telling that in 2011, the U.S. Department of Defense stated “there is no international consensus regarding the definition of a cyber weapon” (Arimatsu). Cyber weapons are generally “computer code that is used… with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings” (Rid 7). Given the absence of international consensus regarding the definition of cyber weapons, the term is better understood based on what it is not rather than what it is. This distinction is subtle, but important legal consequences follow: identifying something as a “weapon” means it may be outlawed and its development, possession, or use may be internationally punishable (Rid 11). Simple malware—for example, theft of personal financial information—has a malicious goal, but demonstrates lower selectivity and wider distribution than a cyber weapon. Additionally, both states and private actors use tools paralleling cyber weapons, but state actors must sponsor a malware in order for it to be a cyber weapon. It is true cyber weapons impact and engage non-state actors to a high degree (Pytlak 40), but state-on-state cyber conflict remains the most common use of cyber weapons, both in terms of increasing severity and frequency (Morgus).

Cyber weapons can be grouped along a spectrum from low-potential to high-potential. Low-potential cyber weapons include malware that can influence a system from the outside, but technically cannot create direct harm. For example, Distributed Denial of Service (DDoS) attacks, where software generates traffic to overload a server, shut down a system without damaging it directly. Some persistent high-volume DDoS attacks have defaced websites and damaged their reputation or caused intellectual property theft. These may cause distressing experiences, but these attacks cause no physical or functional damage to living beings (Rid 8). In contrast, high-potential cyber weapons subtly influence ongoing processes aim to create external physical damage to the targeted system (Rid 9).

From the state’s perspective, the relatively low cost, reduced barriers of entry, and the difficulty in attribution make cyber weapons an attractive option for strategic military and intelligence-gathering operations (Pytlak 3). However, states have fundamentally different interpretations as to what cyber weapons are and what qualifies as acceptable behavior regarding cyber weapon use. States have begun to, and will likely continue to explore possibilities of inflicting physical damage to critical infrastructure via cyber weapons. These new tools present a Cybersecurity issue because state actors often exploit security vulnerabilities in countries’ critical infrastructure in order to initiate attacks. These exploitations create the possibility of physical risk for civilians and place valuable information, including intelligence information or citizens’ private information, at risk of exploitation. The International Strategy for Cyberspace notes all states reserve the right to use military force to respond to electronic attacks, indicating cyber weapons present legitimate physical risks to critical infrastructure and possibly to non-combatant civilians (Anderson).

Policy Problems

Conflicts in cyber space are becoming more prevalent, but states and international institutions have struggled to create framework defining them and restricting their use. According to data collected at New America, 61 cyber attacks have been conducted against other states during peacetime and 24 in wartime since the 1980s (Morgus). Real-world examples of cyber attacks illustrate their technically complex nature that makes it so difficult to attribute actors and create policies curtailing their use. In 2010, the largest known cyber weapon to date, known as Stuxnet, damaged over 1,000 uranium enrichment centrifuges at the Natanz nuclear facility in Iran (Cirenza). Stuxnet was the first time a state, namely the U.S. and Israel, had used cyber weapons to cripple another country’s infrastructure, achieving with computer code what could only be accomplished “by bombing a country or planting explosives” (Sanger). Stuxnet has been described as the “harbinger of a new form of warfare that threatens even the strongest military powers” (Lindsay). Other prominent examples of cyber weapons include Israel launching a cyber-attack that tricked the Syrian air defense system into displaying no approaching airplanes to its operators for a limited time, blinding the entire defense system (Rid 9), and Russia allegedly attacking Ukraine’s power grid in 2016, shutting off lights and heaters for thousands of residents (Zetter).

Currently a “loose amalgamation” of existing international law attempts to govern state action regarding cyber weapons (Morgus). Two international laws in particular regarding behavior in wartime have cyber-specific adaptations*. Jus in bello*, Latin for “right in war,” constricts how states fight, including what assets cannot be targeted and what weapons cannot be used. Three high-level principles underpin *jus in bello*: military necessity, positing an attack must be on a legitimate military target; distinction, the idea combatants must distinguish between combatants and noncombatants; and proportionality, meaning the destruction to civilians and civilian property must be proportional to the strategic gain achieved*.* *Jus ad bellum* defines what kinds of actions constitute an act of war and prescribes what state actions are and are not acceptable during peacetime. In order to wage war, *jus ad bellum* requires a state to have just cause and to declare war—which can only be declared as a last resort.

In 2013, a group of international policy experts released “The Tallinn Manual on the International Law Applicable to Cyber Warfare,” a guidebook interpreting how laws of war, including the principles of necessity, proportionality, and distinction from *jus in bello*, apply to cyberspace (Morgus). The original Tallinn Manual focused on the “most severe” cyber operations, including those that violate the prohibition of the use of force, entitle states to the right of self-defense, or occur during armed conflict (Schmitt). However, as incidences like Stuxnet demonstrate, the reality remains cyber weapons use has become commonplace outside of armed conflict. In response, The Tallinn Manual 2.0 was released in 2017. The updated version adds a legal analysis or “more common cyber incidents” states regularly use and fall below the thresholds of armed conflict or the use of force (“Tallinn Manual Process.”). The updated version is “the most comprehensive analysis of how existing international law applies to cyber operations” (“Tallinn Manual Process.”).

Considerable dispute exists regarding how much International Law matters in practice. Depending on a combination of their view on information security and international laws and legal institutions, states have fundamentally different interpretations as to what cyber weapons are and what is acceptable behavior in regards to their use. For example, China views cyber security as synonymous with “information security,” which encompasses controlling the information available to users online. As such, the Chinese often use cyber weapons against other countries in pursuit of information. In contrast, the United States makes strong distinctions between private industry espionage and espionage through which information critical to national security can be obtained (Pytlak 76). The U.S. is also guided by “equivalence,” arguing they should be able to retaliate cyber attacks through physical means if the magnitude of the attack on the U.S. should warrant it (Pytlak 78). States certainly all have similar interests in protecting critical infrastructure and civilians, but different perspectives from stakeholders mean there are fundamentally different interpretations of the definition of cyber weapons and opinions on how to curtail their use.

Proposed Solution

The ubiquitous nature of cyber weapons and their increase in frequency leaves policy makers and political leaders facing unparalleled challenges in an unfamiliar landscape (Pytlak 98). Despite the likelihood of noncompliance from several countries, creating a new international agreement regarding cyber weapons remains the most effective way to remedy this complex policy issue. This treaty should include a mutually agreed upon definition of what cyber weapons are, outline states’ rights to utilize cyber weapons in peace time, and outline states’ legal obligations to protect critical infrastructure from cyber weapon attacks. Such a treaty would provide a helpful step toward preventing cyber weapons from becoming a tool where customary international law does not apply and states can act freely (Pytlak 15). International legal guidelines around cyber weapons, such as the Tallinn Manual, fail to adequately address cyber threats and it is time for the international community to create a global cyber treaty.

There is evidence to believe an international agreement outlined above would be effective from examining other treaties with a similar purpose as well as states existing interest in creating such a treaty. Cyber weapons are often compared to nuclear, biological, or chemical weapons, which all have respective legal frameworks governing their use (Cirenza). All states, regardless of their strategic interests, have reason to create and ratify such a treaty because it will ensure their actions are in accordance with their international obligations (Pytlak 14). Further evidence supporting this solution comes from states including Russia and China, who have been calling for such a treaty for a number of years. For two countries that strongly advocate for information online to be controlled within their own borders, it is worth questioning their motives (Pytlak 15), but it simultaneously demonstrates the most powerful nations are also vulnerable cyber weapon attacks.

Critics of this solution note that technical difficulties, cultural differences, and varied approaches to the larger cyber realm would realm make the negotiation, adoption, and implementation of such an agreement difficult. Examples of this are ridden throughout even the Tallinn Manual; for example, experts defined a “cyber attack” as one that causes damage to objects, but could not agree on what exactly constituted “damage to objects” (Pytlak 13-14). Additionally, states would likely be interested in working together to address cyber threats posed by non-state actors like terrorists, but they may not be as compelled to constrain their own actions (Valeriano). Given there is currently virtually no global regulation regarding cyber weapons, creating a new treaty dedicated to cyber weapons remains the most effective and compelling policy solution regarding cyber weapons.

Conclusion

Considerable social, political, legal, and technical uncertainties associated with cyber weapons may significantly undermine their revolutionary potential to deter malicious actors internationally without inflicting harm on civilians (Lindsay 365). Examples of cyber weapons are fairly abundant, but despite their prevalence, there is no international consensus among states regarding the definition of a cyber weapon and when it is acceptable to use them. Laws of war have been interpreted to guide cyber weapon use, but these guidelines are not effective in practice due to states’ differing interpretations of cyber weapons. Because cyber weapons present such a unique and novel problem, policy solutions surrounding cyber weapons should focus on creating universal definitions and providing more clarity rather than attempting to apply existing laws of war in a new, unparalleled cyber space. Cyber weapons certainly provide a useful tool for military operations, but they have the potential to create serious harm to civilians and non-combatants if they remain unchecked.

Works Cited

Arimatsu, L. “A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations.” *2012 4th International Conference on Cyber Conflict (CYCON 2012)*. N.p., 2012. 1–19. Print.

Cirenza, Patrick. “Cyberweapons Aren’t Like Nuclear Weapons.” *Slate* 15 Mar. 2016. *Slate*. Web.

Lindsay, Jon R. “Stuxnet and the Limits of Cyber Warfare.” *Security Studies* 22.3 (2013): 365–404. *Taylor and Francis*. Web.

Morgus, Robert. “Rules of Cyber Engagement.” *Slate.* 10 Mar. 2016. *Slate*. Web.

Pytlak, Allison, "Why Do States Use Cyber Weapons? An Empirical Analysis of State-sponsored Cyber Interactions and Rival Dynamics, 2011-2011" (2014). *CUNY Academic Works.*

Rid, Thomas, and Peter McBurney. “Cyber-Weapons.” *The RUSI Journal* 157.1 (2012): 6–13. *CrossRef*. Web.

Sanger, David E. “Obama Ordered Wave of Cyberattacks Against Iran.” *The New York Times.* 1 June 2012. *NYTimes.com*. Web.

Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the Nato Cooperative Cyber Defence Centre of Excellence*, 2013. Print.

“Tallinn Manual Process.” *CCDCOE*. NATO Cooperative Cyber Defense Centre of Excellence. 16 Sept. 2014. Web.

Thomson, Iain. "Snowden: US and Israel Did Create Stuxnet Attack Code." *The Register.* Situation Publishing, 8 July 2013. Web. 01 June 2017.

Valeriano, B. and R.C. Maness. The Dynamics of Cyber Conflict between Rival Antagonists, 2001-11,” *Journal of Peace Research* Vol. 51 (2014), no. 3.

Zetter, Kim. "Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid." *Wired*. Conde Nast, 03 Mar. 2016. Web.