University of Dayton Law Review

Volume 38 | Number 3 Article 4

3-1-2013

Set Computers to Stun: Proposed Cyberwar Rules of Engagement

Jeffrey Greenley
University of Dayton

Set Computers to Stun: Proposed Cyberwar Rules of Engagement

Cover Page Footnote

This article is dedicated to the author's dear mother, who passed away during its formulation. The author also expresses sincere gratitude to Professor Susan W. Brenner, Samuel A. McCray Chair in Law at the University Of Dayton School Of Law for all of her guidance and mentorship during the writing process.

SET COMPUTERS TO STUN: PROPOSED CYBERWAR RULES OF ENGAGEMENT

Jeffrey Greenley[1]

I. INTRODUCTION

In a classic episode of *Star Trek: The Original Series*, Captain James T. Kirk and his crew beam down to the planet Eminiar VII and discover the planet gripped in a 500 year-old-war.[2] To Captain Kirk's surprise, the two factions wage war not with tanks or missiles but with computers and equations.[3] When one side achieves a cyber-hit, the other side receives a computer-generated number of casualties and must terminate that number of its own citizens in "disintegration rooms" or face an actual kinetic retaliation from the other side.[4] Although clearly the planet depicted in Star Trek was a hyperbolic view of future conflicts, twenty-first century war is becoming more and more automated and dependent on computers.[5] As illustrated by the 2008 cyber-attack that occurred in the Eurasian country Georgia, cyber war has become a legitimate threat that must be planned for

---

[1] Comment Editor 2012, Staff Writer 2011, University of Dayton Law Review. J.D., University of Dayton School of Law, 2012; M.E., University of Dayton; B.A. in History Teaching, Brigham Young University. Jeffrey Greenley is an Assistant Attorney General in the Ohio Attorney General's Office and works in the Education Section. He is married to Stephanie Greenley and is the proud father of two children. This article is dedicated to his dear mother who passed away during its formulation. The author also expresses sincere gratitude to Professor Susan W. Brenner, Samuel A. McCray Chair in Law at the University Of Dayton School Of Law for all of her guidance and mentorship during the writing process.

[2] *Star Trek: A Taste of Armageddon* (CBS television broadcast Feb. 23, 1967).

[3] *Id.*

[4] *Id.*

[5] *See* Robert G. Hanseman, *The Realities and Legalities of Information Warfare*, 42 A.F. L. REV. 173, 174 (1997).

by our nation's military.[6] This comment seeks to delineate specific rules of engagement ("ROE") for self-defense to be used by U.S. military forces in the cyber realm and justify those rules in both U.S. and international law.

Section II of this comment will provide a brief history of human warfare, introduce and discuss the purpose of military ROE, give a brief overview of applicable international law, and summarize what the current, unclassified version of the U.S. ROE state.

Section III of this comment will begin with a proposal of what, based on the current state of international law, the ROE for cyber war should be. These rules will be referred to as "proposed cyber ROE." This section will not propose amendments to domestic or international law to better accommodate cyber war. Instead, it will argue that the ROE should be based on current interpretations of international law and past U.S. military precedent.

II. BACKGROUND

The tactics, tools, and laws of warfare have evolved over several centuries of human conflict.[7] Early historical accounts of warfare paint a picture of utter-lawlessness where civilians, women, and children were all targeted in combat along with actual soldiers.[8] Although brutal and lawless wars may have been in early history, modern warfare has been civilized by rigid rules of war and ROE, which attempt to minimize civilian casualties in military conflicts.[9] The earliest accounts of civilizations attempting some regulation of war include the Hindu, which prohibited the use of poison arrows, and early Europeans, who outlawed the crossbow and the arbalest.[10] Later, Hugo Grotius, a well-known Dutch jurist, was influential in crafting European laws of war by insisting on "just causes" for war.[11] His just reasons included crimes against morality, like taking what belonged to

---

[6] Eneken Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE 4 (Nov. 2008), http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf. In 2008 Georgia attacked an uncooperative peacekeeping force that was stationed within their country. *Id.* The attacked group was sympathetic with other Georgians who wished to leave Georgia and reunite with Russia. *Id.* Russia responded with full military force, including a series of cyber-attacks against important Georgian governmental websites. *Id.* These attacks were among the first to be openly sponsored by a nation-state in preparation for a full kinetic military response. *Id.* at 4–5.

[7] *See* Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT'L L.J. 179, 179–80 (2006).

[8] *See generally* William Bradford, *Barbarians at the Gates: A Post-September 11th Proposal to Rationalize the Laws of War*, 73 MISS. L.J. 639 (2004).

[9] *See* Scott D. Sagan, *Rules of Engagement*, *in* AVOIDING WAR: PROBLEMS OF CRISIS MANAGEMENT 443, 444–45 (Alexander L. George ed., 1991).

[10] DOCUMENTS ON THE LAWS OF WAR 29 (Adam Roberts & Richard Guelff eds., 1982).

[11] *See* G.I.A.D. Draper, *Grotius' Place in the Development of Legal Ideas about War*, *in* HUGO GROTIUS AND INTERNATIONAL RELATIONS 175, 194 (Hedley Bull et al. eds., 1992).

others, not keeping your word, or inflicting injury on others.[12]

The U.S. and Europe took some of the most important initial steps towards regulating warfare in the nineteenth century.[13] U.S. historians point to the Union Army's Lieber Code during the Civil War as a major U.S. attempt in constructing ROE to govern commanders during conflict.[14] The code specifically forbade private citizens from being "murdered, enslaved, or carried off to distant parts," and reminded commanders that private citizens were to be "as little disturbed in [their] private relations as the commander of the hostile troops can afford to grant . . . ."[15] A few years later, the European community took further steps towards civilizing war and drafted the Hague Conventions of 1899 and 1907.[16] The Hague Conventions delineated rules to be used on an international level during war on both the land and sea.[17]

Rules of war and ROE have changed and evolved over time to keep up with each new war's strategy and technology.[18] It is extremely difficult for military policy makers to stay ahead of changes between conflicts.[19] Technological changes between World War I ("WWI") and World War II ("WWII") provide an example of this problem.[20] Convinced that any second conflict would be a WWI trench-war, the French constructed an elaborate bunker system on their border with Germany named the Maginot line.[21] Unfortunately for the French, by the time WWII occurred German technology had so advanced that the Germans could either simply fly over the defenses or navigate around the Maginot line's break in the Ardennes Forest.[22] Despite their best efforts, the French were not ready for the type of warfare that this conflict would involve, and as a result, were soon occupied by German forces.[23]

In our modern era, the U.S. military must try to avoid a similar

---

[12] *Id.*

[13] *See e.g.*, DOCUMENTS ON THE LAWS OF WAR, *supra* note 9, at 29; E. D. Townsend, General Orders 100, *in* 3 U.S. WAR DEPARTMENT, THE WAR OF THE REBELLION: A COMPILATION OF THE OFFICIAL RECORDS OF THE UNION AND CONFEDERATE ARMIES, 148–64 (Fred C. Ainsworth & Joseph W. Kirkley eds., 1899).

[14] See Townsend, *supra* note 13, at 148–64, for the complete text of the Lieber Code.

[15] *Id.* at 150–51.

[16] Manley O. Hudson, *Present Status of the Hague Conventions of 1899 and 1907*, 25 AM. J. INT'L L. 114, 114–15 (1931).

[17] *Id.* For a relevant portion of the Hague Conventions, see *infra* note 37.

[18] The Lieber Code, for example, noticed the ever-changing nature of war by stating "[m]odern times are distinguished from earlier ages by the existence at one and the same time of many nations and great governments related to one another in close intercourse." Townsend, *supra* note 13, at 151.

[19] *See* Brown, *supra* note 7, at 179.

[20] *See* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security*, 10 B.U. J. SCI. & TECH. L. 1, 107 (2004).

[21] *See* Christopher Cox, Chairman, SEC, Re-Thinking Regulation in the Era of Global Securities Markets, Speech at the Thirty-fourth Annual Securities Regulation Institute (Jan. 24, 2007), http://www.sec.gov/news/speech/2007/spch012407cc.htm.

[22] *Id.*

[23] *Id.*

mistake and stay one step ahead in both technology and policy in the cyber realm. Current analysts and recent events in Georgia and Egypt suggest that, if or when another conflict starts, the cyber realm will play a major role.[24] Top U.S. military officials concur with this prediction, and in 2002 President George W. Bush signed into law National Security Presidential Directive 16 ("Order 16"), which authorized the U.S. to create cyber ROE.[25] In June 2011, President Obama signed executive orders which reportedly adopted cyber ROE which the Pentagon had created under Order 16.[26] The specific rules of these orders are classified, although the Pentagon did release a small, unclassified version, which discussed broad ROE principles while not giving away any specific strategy.[27] Despite the confidentiality regarding the rules, some U.S. officials have provided an idea of what the classified cyber ROE may contain by publically commenting on them.[28]

A. What are the U.S. ROE?

To begin, what are ROE and what do they govern? U.S. ROE are broad rules promulgated by the Chairman of the Joint Chiefs of Staff to help provide American on-site commanders guidance in both self-defense and mission accomplishment.[29] Sections of the current U.S. ROE that deal with self-defense are mostly unclassified; portions of the latest version were made public in January 2000.[30] ROE dealing with mission accomplishment outline specific guidance for the day-to-day operations of our nation's military in a specific geographic area and are kept confidential.[31] ROE are generally made up of two different categories of rules.[32] The first category is made up of military actions, which can be undertaken by a low-ranking

---

[24] *See supra* note 6 and accompanying text. The Egyptian government collapsed and their President, Hosni Mubarak, was forced to resign after weeks of political unrest and rioting in 2011. David D. Kirkpatrick, *Egypt Erupts in Jubilation as Mubarak Steps Down*, N.Y. TIMES, Feb. 11, 2011, http://www.nytimes.com/2011/02/12/world/middleeast/12egypt.html?pagewanted=all&_r=0. During the weeks of tension, several cyber-attacks were carried out against both the Egyptian government and private Egyptian citizens. *Egypt's Web Disconnect Spurs US Cyber Debate,* CYBERSECURITY NEWS, Feb. 1, 2011, http://cybersecuritynews.org/2011/02/01/egypt%E2%80%99s-web-disconnect-spurs-us-cyber-debate. These attacks climaxed with the Egyptian government being forced to disconnect the Internet to protect themselves and their citizens. *Id.*

[25] Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 128 (2009).

[26] Lolita C. Baldor, *Pentagon Drafts Rules for Cyber Warfare*, CNSNEWS.COM, June 22, 2011, http://www.cnsnews.com/news/article/pentagon-drafts-rules-cyber-warfare.

[27] *See generally* U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE (2011), http://www.defense.gov/news/d20110714cyber.pdf.

[28] Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War*, WALL ST. J., May 30, 2011, at A1, http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html; David E. Sanger & Elisabeth Bumiller, *Pentagon to Consider Cyberattacks Acts of War*, N.Y. TIMES, June 1, 2011, at A10.

[29] Richard J. Grunawalt, *The JCS Standing Rules of Engagement: A Judge Advocate's Primer*, 42 A.F. L. REV. 245, 245 (1997).

[30] CHAIRMAN OF THE JOINT CHIEFS OF STAFF, CJCSI 3121.01A, STANDING RULES OF ENGAGEMENT FOR U.S. FORCES (2000).

[31] Sagan, *supra* note 9, at 444–45.

[32] *Id.* at 444.

battlefield commander under defined circumstances without authorization from higher command.[33] The second category are actions which can be carried out only after express authorization is given by a higher command and govern more violent uses of force or particularly powerful weapons, like nuclear or chemical weapons.[34] Although ROE are developed by the Joint Chiefs and staff judge advocates, they are broad and flexible: the battlefield commander always has the final say in implementing the rules in real-life scenarios, subject to a court-martial should he or she act inappropriately.[35] To summarize, "ROE must ensure that combatants bear only the force necessary to achieve the military objective, engage only necessary targets, [and] discriminate between combatants and noncombatants, and that in doing so they do not cause undue suffering."[36] These broad principles are rooted in both the Hague and Geneva Conventions.[37]

B. Legal Principles of ROE

ROE are deeply rooted in international law.[38] ROE sections that govern self-defense are derived from the U.N. Charter Article 2(4) as well as Articles 39 and 51.[39] Article 2(4) declares that "[a]ll Members shall refrain . . . from the threat or use of force against the territorial integrity or political independence of any state."[40] Alone, Article 2(4) would prohibit *any* force from being used by any nation-state to another, even if that nation-state were provoked.[41] However, subsequent articles of the U.N. Charter condition the absolute prohibition and provide two instances in which a nation-state can retaliate.[42] Article 39 gives the authority for any state to use military force if the Security Council has expressly authorized use of force against that state.[43] Article 39 was used to justify the bombing of Libya by the U.S. in March of 2011.[44] Article 51 provides a second option and states that "[n]othing in the present Charter shall impair the inherent right of

---

[33] *Id.*

[34] *Id.*

[35] 10 U.S.C. § 890(2) (2006); *Id.* at 445.

[36] *See* Mathew Borton et al., *Cyberwar Policy*, 27 J. MARSHALL J. COMPUTER & INFO. L. 303, 313 (2010).

[37] For example, the Hague Convention of 1907 states that "[t]he right of belligerents to adopt means of injuring the enemy is not unlimited" and specifically forbade them from using "arms [or] projectiles . . . calculated to cause unnecessary suffering." DOCUMENTS ON THE LAWS OF WAR, *supra* note 10, at 52. In addition, "the pillage of a town or place . . . [was] prohibited." *Id.* at 53. The Geneva Convention of 1949 further sought to protect civilian casualties stating, "[p]ersons taking no active part in hostilities . . . shall in all circumstances be treated humanely." *Id.* at 273. The Geneva Convention also prohibits civilians from being murdered, taken hostage, or being treated in humiliating or degrading ways. *Id.*

[38] *See* Borton et al., *supra* note 36, at 303.

[39] U.N. Charter arts. 2, para. 4, 39, 51.

[40] *Id.* art. 2, para. 4.

[41] *Id.*

[42] *Id.* arts. 39, 51.

[43] *Id.* art. 39.

[44] Jay Solomon et al., *U.N. Clears Way for Attack on Libya*, WALL ST. J., Mar. 18, 2011, http://online.wsj.com/article/SB10001424052748703818204576206373350344478.html.

individual or collective self-defence," which preserves a nation-state's ability to quickly retaliate against any armed attack as long as that retaliation is attributed to another country; a counter attack is necessary and proportional to the force used against them; and the response is selective in only targeting military as opposed to civilian targets.[45] Article 51 of the U.N. Charter has been interpreted as requiring nations who retaliate in self-defense to only do so out of necessity, in a proportional manner, while distinguishing between military and civilian targets against an attributed attacker.[46]

The principle of necessity requires a nation to respond only to a hostile act or, under the U.S. interpretation, a demonstration of hostile intent.[47] Although a hostile act is typically easy to identify, a demonstration of hostile intent that meets the threshold of allowing a counter-attack is more nebulous.[48] If necessity has been met, a commander's counter-attack must be proportional or reasonable, in terms of intensity, duration and magnitude, required to decisively counter the hostile act of demonstration of hostile intent, but no more than that.[49] If proportionality cannot be achieved, a nation cannot justify an attack under Article 51 and must lobby the U.N. Security Council to either authorize an attack on the aggressive country or, if that fails, seek some other international legal redress.[50] In addition to necessity and proportionality, U.S. forces must use the principle of distinction and distinguish military from civilian targets, carefully launching attacks that would neutralize military capabilities while limiting the collateral damage done to civilians.[51] Finally, a nation must attribute an attack to another country with enough specificity to warrant taking action.[52] These concepts are usually fairly easy to conceptualize in the real world and ROE make canonical guidelines for commanders that vary slightly from theater to theater.[53] However, applying these concepts to the cyber realm has proven to be much more complex.[54] Section III of this comment will

---

[45] U.N. Charter art. 51; Waldemar A. Solf, *Protection of Civilians Against the Effects of Hostilities Under Customary International Law and Under Protocal I*, 1 AM. U. J. INT'L L. & POL'Y 117, 131 (1986).

[46] *See* Borton et al., *supra* note 36, at 312.

[47] Grunawalt, *supra* note 29, at 251.

[48] Sagan, *supra* note 9, at 446–47.

[49] *See* CHAIRMAN OF THE JOINT CHIEFS OF STAFF, CJCSI 3121.01B, STANDING RULES OF ENGAGEMENT/STANDING RULES FOR THE USE OF FORCE FOR U.S. FORCES (2005).

[50] U.N. Charter arts. 39, 51.

[51] Borton et al., *supra* note 36, at 313.

[52] Charles J. Dunlap Jr., *Perspective for Cyber Strategists on Law for Cyberwar*, 5 STRATEGIC STUD. Q. 81, 88 (2011).

[53] Sagan, *supra* note 9, at 445.

[54] For example, would a proportional response to a denial of service ("DoS") attack by a nation-state on the U.S. be to attack that computer with a DoS attack or to use something that would either physically or electronically destroy its ability to function? Could the Internet cables under the ocean supplying access to that computer be severed? Could the civilian or state Internet service provider's buildings responsible for providing Internet access be destroyed by a cruise missile? These are all questions that are to be discussed in this comment.

analyze proposed cyber ROE and justify them under each of the aforementioned legal principles.

C. Types of Cyber-weapons

Where normal warfare uses weapons like missiles, guns, tanks, and airplanes, cyber war employs its own variety of cyber-weapons.[55] Some cyber-weapons only temporally disrupt a computer's functions.[56] A Denial of Service ("DoS") attack uses thousands of computers to overwhelm a system's server by simultaneously trying to access it.[57] This type of attack is inexpensive and can disrupt a website's ability to perform its function for a short period while not actually destroying a system.[58] Another concept related to a DoS attack is a "zombie" or bot computer.[59] These computers are nicknamed "zombie" because they are owned and operated by an individual or group, but have been hijacked by an attacker and used in coordination with other computers, usually a coordinated DoS attack, to disrupt a website against their actual owner's will.[60] These attacks can be so devastating that they result in the complete destruction of hardware, which must be reinstalled before a computer can recover.[61]

Other cyber-weapons, however, are more destructive.[62] There are whole hosts of malicious software that, once activated, can disrupt a computer's ability to perform a task or provide others with access to its files.[63] One commonly known type, a virus, spreads across a network by replicating itself within a system.[64] Once it has grown to a sufficient size it performs a task that either corrupts a system or destroys important sensitive data needed for the computer to function.[65] A worm is similar to a virus but in addition to the ability to perform a task, it replicates itself until a computer's memory or server can no longer perform any function.[66] At the same time, a worm also keeps open a doorway to provide an outside assailant access to the system's files.[67] Finally, cyber warriors have recently invented the more sophisticated StuxNet worm.[68] This weapon is different than traditional worms because it can target a specific type of computer and

---

[55] *See* Schaap, *supra* note 25, at 134. Much of this section is made possible by Major Schaap's excellent research and ability to help non-technology users understand complex cyber-weapons.
[56] *Id.* at 172.
[57] *Id.* at 134.
[58] *Id.*
[59] *Id.*
[60] *Id.*
[61] *Id.* at 135.
[62] *See id.*
[63] *Id.*
[64] *Id.*
[65] *Id*. at 135–36.
[66] *Id.* at 136.
[67] *Id.*
[68] Daniela Oliveira, *Cyber-Terrorism & Critical Energy Infrastructure Vulnerability to Cyber-Attacks*, 5 ENVTL. & ENERGY L. & POL'Y J. 519, 526 (2010).

avoid all others.[69] In 2010, this worm infected an Iranian nuclear power plant and caused critical centrifuge components to destroy themselves and, in one analyst's opinion, set Iran's nuclear program back by two years.[70] The cyber-weapons discussed above are not an exhaustive list; they are merely the more commonly used weapons in cyberspace.[71] It is impossible to describe *every* weapon at a nation-state's disposal, as they are constantly being created by groups around the world.[72]

It is thus imperative, given the history and necessity of always staying one step ahead in war, for the U.S. to seriously analyze and establish ROE for the cyber realm as soon as possible. The issue, however, is what will the cyber ROE allow while complying with the legal self-defense principles of ROE: necessity, proportionality, attribution, and distinction.[73] In addition, a threshold issue on establishing ROE is whether the military even has jurisdiction at all in helping police cyberspace.[74] In the following section the reasons for allowing military jurisdiction in cyberspace will be introduced and substantiated, and this comment's proposed cyber ROE will be articulated and then justified under now existing rules of war.[75]

III. ANALYSIS

A. Who Has Jurisdiction, the Military or Law Enforcement?

A threshold issue in cyber war is whether the military should have jurisdiction in the cyber arena or if it would be better left to some other entity. There are various opinions on whether the U.S. military has jurisdiction, which branch of the military would lead the defense if attacked, or if cyber war is better left to the FBI or some other contracted entity.[76] The argument revolves around the Posse Comitatus Act, an act that prohibits

---

[69] *Id.*

[70] Yaakov Katz, *Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years*, JERUSALEM POST, Dec. 15, 2010, http://www.jpost.com/LandedPages/PrintArticle.aspx?id=199475.

[71] *See* Schaap, *supra* note 25, at 134. The United States military understands that weapons are being constantly developed and have created a way for new military cyber-weapons to have a legal review before being used. *See, e.g.*, SEC'Y OF THE AIR FORCE, AIR FORCE INSTRUCTION 51-402, LEGAL REVIEWS OF WEAPONS AND CYBER CAPABILITIES (2011), http://www.fas.org/irp/doddir/usaf/afi51-402.pdf (prescribing guidelines and procedures for review of Air Force weapons and cyber capabilities to ensure legality under domestic and international law).

[72] For example, as this paper was being prepared for press a new variation of the StuxNet virus had been discovered, nicknamed Duqu. William Jackson, *Son of Stuxnet Could Usher in a New Chapter in Cyber Warfare*, GOVERNMENT COMPUTER NEWS, Nov. 4, 2011, http://gcn.com/articles/2011/11/07/cybereye-duqu-raises-cyberwar-stakes.aspx.

[73] *See* discussion *infra* Part III.B.

[74] *See* discussion *infra* Part III.A.

[75] *See* discussion *infra* Part III.A–B.

[76] *See, e.g.*, Dunlap, *supra* note 52, at 84 ("If [an attack] is truly 'war,' then a response under a national-security legal regime is possible; if not, then treating the matter as a law enforcement issue is appropriate."); *see also* Adam Ebrahim, *Going to War with the Army You Can Afford: The United States, International Law, and the Private Military Industry*, 28 B.U. INT'L L.J. 181, 184 (2010) (advocating the use of private mercenaries in cyber war).

military involvement in criminal investigation, which was passed shortly after Reconstruction to ensure that the U.S. Army would never have the police powers it held during that era in the South.[77] Those who support a law enforcement response to cyber-attacks might argue that if a cyber-attack occurs, it will not likely target U.S. military facilities, but private businesses like banks, power stations, or other important pieces of infrastructure. They suggest that the military does not normally respond to criminal acts of destruction, especially to a civilian building, and thus, the military should not respond in cyberspace either.[78] A law enforcement response is also appealing since both nation-states and private individuals wage cyber war.[79] Because the military cannot attack private citizens, proponents of a law enforcement model suggest that law enforcement must be allowed to police the cyber arena.[80] Finally, they argue that a law enforcement response would solve the issue of whether the military can wage war on non-nation-states in general.[81]

Despite these arguments, the U.S. military must have jurisdiction in cyberspace and the Posse Comitatus Act does not apply to the cyber arena. There are important policy reasons to support military involvement in the cyber arena. For example, local law enforcement, and even the FBI, likely lack the funding and expertise to combat certain cyber-attacks.[82] In addition, the U.S. cannot afford to trust the protection of its important national cyber resources to small groups across the country with no centralized decision-making ability. At the same time, nation-states and other hostile groups who seek to destroy U.S. cyber assets would not be deterred by the possibility of criminal sanctions which law enforcement provide. This is especially true given the Supreme Court's extension of both habeas corpus and due process rights to non-citizen enemy combatants.[83]

---

[77] 18 U.S.C.A. § 1385 (West 2009). For a number of resources explaining why the Posse Comitatus Act was passed and what kinds of acts it was designed to prevent, see Brian L. Porto, *Construction and Application of Posse Comitatus Act (18. U.S.C.A. 1385), and Similar Predecessor Provisions, Restricting Use of United States Army and Air Force to Execute Laws*, 141 A.L.R. FED. 271 (1997). For an excellent article reviewing Posse Comitatus issues in cyberspace see Sean M. Condron, *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 403 (2007).

[78] *See* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/terrorism/warfare*, 97 J. CRIM. L. & CRIMINOLOGY 379, 414 (2007). Professor Brenner does an excellent job in an article of explaining the history of law enforcement, its evolution, and how there is historical precedent for some law enforcement jurisdiction in cyberspace.

[79] *Id*. at 435–36.

[80] *See id.* at 458.

[81] *See id. See generally* Brown, *supra* note 7. For another source advocating for law-enforcement in cyber war, see Carolyn W. Pumphrey, *Introduction* to TRANSNATIONAL THREATS: BLENDING LAW ENFORCEMENT AND MILITARY STRATEGIES 1, 1–2 (Carolyn W. Pumphrey ed., 2000).

[82] That is not to say that these groups are not highly skilled in their normal day-to-day operations but only that they lack the expertise in the cyber arena. Arguably, the most skilled and well-founded groups that could respond to a cyber-attack are not the military but specialized private companies like Microsoft or Google who deal with these kinds of attacks on a daily basis.

[83] Boumediene v. Bush, 553 U.S. 723, 795 (2008) (holding that alien enemy combatants held at Guantanamo Bay prison were entitled to seek a writ of habeas corpus); Hamdi v. Rumsfeld, 542 U.S.

Under those holdings, enemy combatants can safely target U.S. cyber assets while being assured that if they are caught and extradited by law-enforcement, they will be given a lawyer and provided some of the protections the U.S. Constitution provides to its citizens.[84] Therefore, only the promise of a swift military cyber counter-strike will deter cyber-attackers from carrying out their plans.

The success that has followed from the recent shift in military jurisdiction over some terrorist acts supports the conclusion that the military must have an involved role in cyber conflicts.[85] In President Bush's recent memoirs, he made a poignant observation about terrorism and its shift from a criminal matter to one controlled by the military: "[o]n 9/11, it was obvious the law enforcement approach to terrorism had failed. Suicidal men willing to fly passenger planes into buildings were not common criminals. They could not be deterred by the threat of prosecution."[86] After the 9/11 attacks, the U.S. military began to wage war on terrorism and to protect the nation from a threat that was deemed too large to be handled by local law enforcement.[87] The fact that the U.S. has successfully deterred any major terrorist attack on U.S. soil since that jurisdictional shift is proof of success in allowing the military to deal with some threats traditionally dealt with by law enforcement.[88]

In addition to strong policy reasons to support a military role, on its face the Posse Comitatus Act does not apply to military jurisdiction in cyberspace and thus cannot prevent the military from engaging in law enforcement. Canons of statutory construction illustrate why the Act does not apply in this situation. First, the Act cannot be found to prevent military cyber jurisdiction since the original purpose of the statute was to prevent the kind of military occupation that took place in the South during Reconstruction from occurring in the future.[89] Thus, the Act only prohibits Reconstruction-like law enforcement activities, and cyber threats are simply not the kind of law enforcement activities that the Act was designed to prohibit.[90] Opponents to this argument might argue that military involvement in cyberspace would, in actuality, create an occupation of cyberspace by a military force that is indistinguishable from those that took place during the Reconstruction era. However, that argument would fail

507, 539 (2004) (holding that non-citizen detainees held at Guantanamo Bay prison are entitled to some due process rights).

[84] *See Boumediene,* 553 U.S. at 795*; Hamdi*, 542 U.S. at 539.

[85] *See* GEORGE W. BUSH, DECISION POINTS 154–57 *(*2010).

[86] *Id.* at 154.

[87] *Id.*

[88] Rick Newman, *How America has Underperformed Since 9/11*, U.S. NEWS & WORLD REP., Sept. 7, 2011, http://www.usnews.com/news/blogs/rick-newman/2011/09/07/how-america-has-underperformed-since-9-11.

[89] *See* United States v. Allred, 867 F.2d 856, 870–71 (5th Cir. 1989).

[90] *See id.*

because, unlike the Reconstruction era where commanders essentially made any decisions necessary to protect freedmen,[91] the military would not even have jurisdiction in cyber war unless certain conditions were present, as discussed below.[92] That check would ensure that the military would clearly understand when and how it would have jurisdiction to protect the U.S. from cyber threats and prevent the carte blanche authority given during Reconstruction.[93]

Even if a court were to construe the Act as prohibiting a military presence in cyberspace, the plain language of the statute only lists the Air Force and Army as being prohibited from assisting in law enforcement; the Navy is not listed and thus could engage in cyber law enforcement acts legally.[94] This argument is currently limited, as the Department of the Navy has promulgated regulations that place the Navy within the prohibition set by the Posse Comitatus Act.[95] However, because these are only regulations they could easily be repealed.[96] In addition, the plain language of the Navy regulation allows high-level officials to override the regulation and allows law enforcement efforts under certain circumstances.[97] That specific clause was used to allow the Navy to assist law enforcement efforts in the U.S. War on Drugs.[98] These canons of construction arguments, combined with the aforementioned policy arguments, would likely convince a court to allow military jurisdiction, or pressure Congress to modify the Posse Comitatus Act and allow military control of some law enforcement acts in cyberspace, given their unique threat.[99]

Thus, although the military clearly should not have a blank check to defend against every cyber-attack, the U.S. must allow the military jurisdiction to defend or respond to cyber-attacks against specific entities, such as power plants or key financial institutions, as they are important

---

[91] *See* Detlev F. Vagts, *Military Commissions: The Forgotten Reconstruction Chapter,* 23 AM. U. INT'L L. REV. 231, 238 (2008).

[92] *See infra* text accompanying note 100.

[93] *See* Condron, *supra* note 77, at 419.

[94] United States v. Yunis, 924 F.2d 1086, 1093 (D.C. Cir. 1991); Schowengerdt v. Gen. Dynamics Corp., 823 F.2d 1328, 1340 (9th Cir. 1987), *abrogated by* Pollard v. GEO Group, Inc., 629 F.3d 843, 854 (9th Cir. 2010), *rev'd sub nom* Minneci v. Pollard, 132 S. Ct. 617 (2012).

[95] United States v. Walden, 490 F.2d 372, 374 (4th Cir. 1974); Borton et al., *supra* note 36, at 323.

[96] Borton et al., *supra* note 36, at 323. Unlike statutes passed by Congress, which must be formally repealed by the consensus of both houses, rules promulgated by agencies, like the Department of the Navy, can quickly be eliminated by their own agency in lieu on a former vote by Congress. *Id.*

[97] Gary Felicetti & John Luce, *The Posse Comitatus Act: Setting the Record Straight on 124 Years of Mischief and Misunderstanding Before Any More Damage Is Done*, 175 MIL. L. REV. 86, 149 (2003).

[98] *Id.* at 148. For a discussion of other instances in which the Posse Comitatus Act has been avoided, see Geoffrey Klingsporn, *The Secret Posse: Behind the Veil of National Security, Information Warfare Is Eclipsing the Difference Between Military and Domestic Affairs*, LEGAL AFF., March/April 2005, at 23–24.

[99] However, given Congress's slow moving nature, this is not likely to occur until some type of large-scale cyber-attack is launched against the U.S. which forces Congress to react and take action.

centers of national security.[100] Therefore, under this comment's ROE, any attack against power plants, Executive or Congressional computer networks, or key financial systems, would warrant a military, as opposed to a law-enforcement, response.[101] All other attacks, including those on civilian internet service providers ("ISPs"), would have to be protected by either their own security force or some other law enforcement group, since those attacks would go beyond military jurisdiction as they do not relate to national security.[102]

B. Proposed Cyber ROE for the U.S. Military

Because the military must have jurisdiction over some cyber-attacks, this comment proposes specific ROE to govern them. Military commanders would be able to deploy low-level weapons capable of temporarily stunning enemy computer systems, regardless of complete attribution and without authorization from command. In addition, commanders could deploy these stun cyber-weapons as a direct response to an enemy's actual attack or to prevent an enemy's imminent use of cyber-weapons capable of causing real-world physical destruction, as long as a commander has credible intelligence of that attack. No duty to warn would apply in cyberspace. These weapons could target attacking computers individually, or if reasonably attributed to a nation-state or group, dual-use buildings such as power plants.

However, it is clear that in the event of a large-scale attack, the U.S. military might have to use large-scale cyber or kinetic weapons that could permanently destroy a computer system. Although the necessity element remains the same, a commander could only use weapons if he or she has reasonably attributed a system or group as being responsible for an attack and if authorization from a higher command has been given prior to deploying those weapons. The next four sections of this comment will further expand these proposed rules and justify them under the self-defense principles of necessity, proportionality, distinction, and attribution.

---

[100] *See* Gorman & Barnes, *supra* note 28. A U.S. military official agreed with this statement and remarked, "[i]f you shut down our power grid, maybe we will put a missile down one of your smokestacks." *Id.* Defining what is and what is not an important center of national security will be discussed below. *See infra* text accompanying notes 101–02, 162–65. It would appear that the Pentagon would agree with this comment, having stated publically that it would launch cyber-weapons in response to "significant cyber attacks directed against the U.S. economy, government or military." Ellen Nakashima, *Pentagon: Offensive Cyber Attacks Fair Game*, WASH. POST, Nov. 15 2011, http://www.washingtonpost.com/blogs/checkpoint-washington/post/pentagon-offensive-cyber-attacks-fair-game/2011/11/15/gIQAxQlcON_blog.html.

[101] Discerning what is and what is not a system valuable to national security is increasingly difficult. The U.S. and the World are increasingly inter-connected by technology and lines delineating important systems become thinner as technology continues to advance.

[102] ISPs are interesting because there is arguably nothing more important to national security than these companies. They are not included in this comment's definition simply because it is assumed that because they provide internet service, they likely have their own sophisticated anti-cyber-attack systems in place.

1. Necessity

When will a cyber-presence or cyber-attack reach the necessity threshold and allow a military response? Article 51 of the U.N. Charter only allows a nation to attack another in self-defense if it is necessary to do so.[103] Necessity only allows the military to respond to a hostile act, or an intention to commit a hostile act, by another.[104] Major Dunlap, a well-known cyber war strategist, suggests that an effects-based analysis should be used to determine whether or not an act is hostile.[105] He suggests that if a cyber-attack has the effect of destroying something in the real world, it is a hostile act under the U.N. Charter, and the U.S. would be allowed to respond.[106] Thus, under Major Dunlap's theory, the transmission of a destructive worm or virus that leads to destruction in the physical world, like the StuxNet virus did in destroying actual real-world Iranian property, is an armed attack that would warrant a military response.[107] Any response would have to be justified under the other U.N. self-defense principles, but the necessity element would be met.[108] This comment's proposed cyber ROE adopts this standard and would allow a commander to respond to any cyber-attack that physically destroys property or data. Those attacks that would only temporarily disable a system or provide a backdoor into sensitive data would not be an armed attack and would not allow a military response.[109]

In addition to responding to actual hostile acts, the military must

---

[103] U.N. Charter art. 51.

[104] *See* Grunawalt, *supra* note 29, at 251. An aspect upon which most legal commentators agree relates to cyber efforts to steal information; espionage has never been regarded as the use or threat of use of force, let alone a hostile act. Duncan Blake & Joseph S. Imburgia, *"Bloodless Weapons"? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining Them as "Weapons,"* 66 A.F. L. REV. 157, 186 (2010). Thus, should the allegations of China stealing U.S. technology ever prove true, the U.S. could not mount any kind of military response under current law. Jeremy Page, *Stealth-Espionage Claims Disputed in China*, WALL ST. J., Jan. 26, 2011, at A16.

[105] Dunlap, *supra* note 52, at 85. Other scholars argue that an instrument-based approach, where one looks at whether any existing kinetic weapon could have done the damage, and if it could, then it should be considered as a hostile act. Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 54–55 (2009). Others suggest a strict-liability approach where *any* cyber-attack would be treated as an armed attack. *Id.* at 55.

[106] Dunlap, *supra* note 52, at 85.

[107] *Id.* ("The leading view, therefore, among legal experts focuses on the consequences and calls for an effects-based analysis of a particular cyber incident to determine whether or not it equates to an 'armed attack' . . . .") (emphasis omitted). Not all legal commentators agree with this idea and some argue that because a cyber-attack is not a physical one the rules of war would not apply at all. Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts*, 43 VAND. J. TRANSNAT'L L. 1011, 1031 (2010) ("Since cyber[-]attacks will almost certainly not involve the use of physical force, the Charter and the contemporary LOAC probably do not apply. If the LOAC does not apply to cyber[-]attacks, a country would not commit an illegal act by deliberately launching such attacks at civilian-owned targets; this distinction makes offensive cyberwarfare an attractive option for aggressive nation-states.").

[108] Gorman & Barnes, *supra* note 28, at A1. The Wall Street Journal reported that this idea is favored by the Pentagon and is likely in the confidential Cyber ROE not available publically. *Id.*

[109] Dunlap, *supra* note 52, at 85 (stating that consequences must extend to more than mere inconvenience; there must be at least temporary damage of some kind). This is the kind of situation where a law enforcement response would be more appropriate.

also be allowed to respond to an intention to commit a hostile act before it occurs. This doctrine is also sometimes referred to as anticipatory self-defense.[110] But what does a demonstration of hostile intent that would warrant anticipatory self-defense look like in the cyber realm? Using the above transmission of the StuxNet virus as an example, at what point could the U.S. military interpret hostile intent and stop the virus from being transmitted before it reaches the system? Must the military wait until the virus has been transmitted into a system and is about to be implemented before responding? Could it attack as soon as a foreign computer is found trespassing in the network,[111] or, could it launch a preemptory attack as soon as a nation-state or group announces it is funding the creation of the cyber-weapon? To further complicate the matter, not all interpreters of the U.N. Charter agree that *any* demonstration of hostile intent can warrant a military response.[112] Those who argue against it state that unless an act is done in conjunction with an actual attack, no response can occur.[113]

Despite this argument, the U.S. must continue to launch anticipatory self-defense attacks to protect itself.[114] In many ways, anticipatory self-defense makes sense. For example, the Model Penal Code ("MPC"), a respected body of legal literature, defines self-defense as "the use of force upon or toward another person is justifiable when the actor believes that such force is immediately necessary for the purpose of protecting himself against the use of unlawful force by such other person on the present occasion."[115] Under the MPC, one does not have to simply wait to be hit before protecting oneself, rather as long as an actor believes that force is immediately necessary to stop harm from occurring, he or she is justified in stopping the attack before it begins.[116] Although the MPC does not apply in this arena, it supports the idea that U.S. forces cannot wait to receive a black eye before acting; they must prevent the blow from occurring at all.

But at what point is an anticipatory attack justified? Under current ROE, a foreign plane flying into U.S. airspace without authorization does not meet the threshold of a demonstration of hostile intent and it cannot

---

[110] Matthew Hoisington, Comment, *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, 32 B.C. INT'L & COMP. L. REV. 439, 450 (2009).

[111] Schaap believes that trespass alone in a computer network is not enough to warrant a response. Schaap, *supra* note 25, at 143. *But see* W. Earl Boebert, *A Survey of Challenges in Attribution*, *in* NAT'L RES. COUNCIL OF THE NAT'L ACADEMIES, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS 41, 42 (2010) (arguing that if a specific IP address can be found several different times in a system "scouting the building" then that action could be interpreted as a demonstration of hostile intent and a counter-attack could occur to stop that IP address from entering again).

[112] Dunlap, *supra* note 52, at 86.

[113] *Id.* at 87.

[114] As an example of why anticipatory self-defense in important, in 1987 the *USS Stark* was sunk by an Iraqi Mirage F-1 aircraft because the frigate waited too long in determining whether or not the aircraft had met the threshold of hostile intent. Sagan, *supra* note 9, at 456–58.

[115] MODEL PENAL CODE § 3.04 (1962).

[116] *Id.*

simply be destroyed.[117] This translates to the cyber realm as not allowing the military to target a computer that is merely trespassing in a system.[118] In the same way, when an enemy aircraft flying close to an armed aircraft carrier or civilian instillation opens up its bombing doors, it has done enough to show hostile intent and, if it refuses to stand down, it can be fired upon.[119] Therefore, under this comment's proposed cyber ROE, the uploading of a virus or other cyber-weapon is the equivalent of the opening of an airplane's bombing doors and the military would be free to respond to that threat. The proposed cyber ROE, however, goes one step further and would allow a commander with *credible* intelligence of *imminent* use of a cyber-weapon capable of causing destruction in the physical world to launch an anticipatory self-defense, if authorized by higher officials.[120] Intelligence alone that a weapon is being developed, however, would not be a demonstration of hostile intent sufficient to allow the military to attack the laboratory.[121]

There is one final issue with anticipatory self-defense in cyberspace: the duty to warn.[122] Under current ROE, a commander must warn an incoming entity that it is in violation of U.S. sovereignty and, if it continues, it will be interpreted as a threat and fired upon.[123] However, in cyberspace, the military is not only unaware of whom the enemy is, but also lacks clear communication channels to make contact.[124] Thus, due to the rapid speed under which cyber-attacks occur and an inability to have clear communication to the one or thousands of attacking systems, there cannot

---

[117] Sagan, *supra* note 9, at 446.

[118] Of course, this is also fact sensitive as the mere presence of an aircraft in restricted airspace, like the space above the White House, is a demonstration of hostile intent and would warrant a response. *See id*. at 452. The question then is what types of computer networks, if any, are so crucial to national security that mere presence could warrant a cyber-response? Aside from portions of the U.S. Military or State Department confidential files databases and perhaps nuclear power plants, no system would seem to be the equivalent of the White House and thus worthy of similar protection.

[119] *Id.* at 446.

[120] This standard is based off of the one currently used by the U.S. military as stated by Sagan. *Id.* at 447. However, unlike the traditional standard, which only allows an anticipator attack if it is "beyond reasonable doubt" than an attack will occur, the proposed cyber ROE only uses a "credible" standard. *Id.* This is due to the aforementioned problem of attack speed in cyberspace. A commander cannot wait to ascertain beyond a reasonable doubt, at least in using stun weapons. As mentioned later in the article, those weapons which are more destructive cyber or kinetic weapons must be fully attributed and authorized before being use. *Contra* Dunlap, *supra* note 52, at 87 ("[I]t may behoove cyber strategists to avoid embracing a legal interpretation that would categorize the nondestructive insertion of a cyber capability into the computer system of another nation as either a use of force or an armed attack. The better view today would be that such activities—without an accompanying intent for imminent action—would not be uses of force, so long as the cyber capability lies dormant.").

[121] As this article heads to press, unnamed sources in the Pentagon suggested that the U.S. had already decided that anticipatory self-defense, or pre-emptive strikes, were authorized under confidential orders. *See* Nikhil Kumar, *US Draws up Battle Plan to Stave Off Digital Attack Cyberstrikes*, THE INDEPENDENT, Feb. 4, 2013, http://www.independent.co.uk/news/world/americas/us-draws-up-battle-plan-to-stave-off-digital-attack-cyberstrikes-8480656.html.

[122] Sagan, *supra* note 9, at 452.

[123] *Id.*

[124] It would be absurd to force the military to IM, text or email an assailant to warn them to cease and desist.

be a duty to warn in cyberspace. The proposed cyber ROE would remind commanders that, due to the inability to warn, extra caution should be used before launching a cyber counter-attack.[125]

2. Proportionality

If an attack is necessary, the current interpretation of Article 51 of the U.N. Charter only allows a proportional military counter-attack.[126] Proportionality requires a military response to be reasonable in both duration and breadth to counter the hostile act.[127] Applying this rule to the cyber realm, the military cannot use a small computer attack to justify destroying an entire nation, either physically or electronically. Instead, a nation can only respond with cyber-weapons that would reasonably and decisively counter the initial hostile act.[128] Under this comment's proposed cyber ROE, a cyber-attack which would reach the level of an armed attack could always be countered by using U.S. cyber-weapons which would only stun a system and prevent in it from being used any further. How to respond and what choice of cyber-weapon to use in that kind of situation would be decisions that battlefield commanders could make under the cyber ROE's guidelines without authorization, and *only* to the extent necessary to counter the hostile act.[129]

The use of stun attacks without authorization is supported by the fact that those weapons would normally fall below, not only the armed attack threshold of Article 51 of the U.N. Charter, but also the use of force threshold under Article 2(4).[130] Article 2(4) prohibits the use of force against other nations.[131] If an attack is not a use of force, then a military can employ that technique without fear of consequences.[132] The U.N. recently held that stun cyber-weapons fall below the use of force threshold.[133]

---

[125] Despite an inability to warn, it could be possible to launch a "shot across the bow" to warn attackers that they have been discovered and to desist in their assault. An example could be launching a small DoS attack on the originating system while they are in your system to let them know that they have been discovered and to leave immediately. The military could also repeatedly ping the incoming IP address to let them know that they have been discovered. While these would be good practices, the speed that cyber-attacks occur makes it impractical to do so.

[126] U.N. Charter art. 51; *see also* Sklerov, *supra* note 105, at 32–33.

[127] Grunawalt, *supra* note 29, at 251.

[128] *Id.*

[129] Current policy supports this idea and would allow a battlefield commander to respond to a cyber-attack with cyber-weapons without authorization from command. For example, if a platoon of military soldiers were suddenly fired on they would not have to radio command for authorization to engage those people firing at them. However, because un-authorized attacks could cause explosive political issues, only low-level weapons could be used without authorization. However, due to attribution issues to be discussed later in this comment, caution must rule the day when using a kinetic weapon response.

[130] *See* Brenner & Clarke, *supra* note 107, at 1031.

[131] U.N. Charter art. 2, para. 4.

[132] After all, the U.N. Charter only applies to the "use or threat of force." *Id.*

[133] Schaap, *supra* note 25, at 143. As an example, the DoS attacks recently suffered by Estonia by un-attributed assailants were not found meet the use of force threshold. *Id.* at 144. Blake, another well-known cyber strategist, agrees, stating:

Giving a battlefield commander the flexibility to counter a real-world fast attack without authorization by stunning an enemy system would protect U.S. interests while limiting the probability of breaching international law.[134]

What types of attacks would justify using more destructive cyber-weapons or actual kinetic weapons? Cyber-attacks could rise to an incredibly destructive level and, when they occur, happen very quickly. The proposed cyber ROE give commanders flexibility in quickly countering a large-scale attack with stun weapons without contacting command for authorization. However, if large-scale or kinetic weapons are truly needed to physically destroy an attacking system, their use must be authorized by a higher official before being used due to its destructive force and, again, *only* used as necessary to counter the hostile act. To gain authorization, a battlefield commander would have a heightened attribution requirement before deploying kinetic weaponry, as discussed in the next section.

3. Attribution

Current interpretations of the U.N. Charter require a counter-attack to be attributed to some nation or group before being launched.[135] Attribution has been referred to as the "single greatest challenge to the application of the law of armed conflict to cyber activity."[136] Traditional military attacks are generally easy to attribute. In traditional warfare, weapons are so elaborate and expensive that typically only nation-states can afford them.[137] These expensive weapons of war are then loaded on to even more expensive planes or ships, resplendent with battle flags or other patriotic symbols, to be used in battle.[138] Those symbols and flags are then used to attribute an attacker. Even if an attacking force were unmarked, it is easy to deduce a small number of probable suspects; only a few nations in

---

> [o]ne State's use of bloodless capabilities with negligible effects in scale and gravity in another State, especially if the effects are not directed at that State, is unlikely to amount to a 'threat or use of force against the territorial integrity or political independence' of that State, even if a military force is operating the capability.

Blake & Imburgia, *supra* note 104, at 187.

[134] However, just because an attack would not rise to the level of an armed attack should not give the U.S. military carte blanche authority to attack on a whim. Clearly the U.S. military has a strong public relations reason for being careful in how freely they attack others.

[135] Levi Grosswald, Note, *Cyberattack Attribution Matters Under Article 51 of the U.N. Charter*, 36 BROOK. J. INT'L L. 1151, 1164 (2011).

[136] Dunlap, *supra* note 52, at 88 (quoting Todd C. Huntley, *Controlling the Use of Force in Cyberspace*, 60 NAVAL L. REV. 1, 34 (2010)). Levi Grosswald recently wrote an excellent note discussing the problem of online attribution and the various ways to solve. *See generally* Grosswald, *supra* note 135.

[137] Most individuals or groups, no matter how wealthy, cannot afford cruise missiles, aircraft carriers or any of the other weapons of war.

[138] Interestingly, the Hague Convention only applies to belligerents who have a "fixed distinctive emblem." Michael N. Schmitt, *Bellum Americanum: The U.S. View of Twenty-First Century War and Its Possible Implications for the Law of Armed Conflict*, 19 MICH. J. INT'L L. 1051, 1078 (1998).

the world can afford large planes with large payloads to launch elaborate attacks.[139]

In cyberspace however, anyone with a computer could be sending an attack without any kind of identifying information, although a particularly sophisticated cyber-weapon does give a large implicit inference of *some* state involvement.[140] Software is generally cheap to create, easy to share, and if deployed correctly, just as dangerous as a normal, kinetic weapon.[141] Where before civilians or smaller groups of people could not afford to wage war against a nation-state, they can now enter the arena and cause devastation, thereby complicating the U.S. military's ability to confidently attribute where an attack is coming from.[142]

To further complicate attribution, attacking computers can mask their location and prohibit an aggrieved country from identifying them.[143] Attackers can either make it look as if their computer is somewhere it is not, or is precisely where indicated but under the control of an assailant thousands of miles away.[144] It is extremely difficult for a nation to attribute an attack to an attacker that is invisible or is lying about its location.[145] Thus, in the cyber realm, particularly with zombie computers or IP masking, one can almost never be completely sure who is attacking.[146] Despite these issues, the proposed cyber ROE would allow the use of stun cyber-weapons to fire back and disable a computer's ability to fight without complete attribution, since those attacks would not destroy a system but instead disable it.

But what if an attack were longer in duration or had physically destroyed U.S. property? The proposed cyber ROE would force the military to meet a higher reasonable-assurance attribution requirement before deploying more destructive cyber-weapons. The use of conventional arms, however, would have to meet a nearly complete attribution requirement before being deployed. The possibility of a U.S. military response that destroyed either domestic or foreign personal property without being completely attributed is extremely dangerous. The military cannot respond too quickly with something that could be interpreted as an act of war. However, if an attack were so overpowering that legitimate U.S. interests

---

[139] *See* Grosswald, *supra* note 135, at 1166–67.

[140] *See* Nancy McKenna, *Stuxnet: The First Cyber "Super-Weapon?,"* 6 No. 11 QUINLAN, COMPUTER CRIME AND TECH. IN L. ENFORCEMENT, Nov. 2010, at art. 5.

[141] *See* Condron, *supra* note 77, at 404.

[142] *See* Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VAND. J. TRANSNAT'L L. 57, 83 (2010).

[143] Grosswald, *supra* note 135, at 1169.

[144] Imagine the chaos that could ensue if an attacker were to attack the Kremlin using hacked computer systems from the pentagon. If a Russian response were to destroy a U.S. system, war could quickly ensue.

[145] *See* Grosswald, *supra* note 135, at 1166–68.

[146] *Id.* at 1168.

were at stake and important property could be physically destroyed, the ROE would give authority, with a reasonable level of attribution and authorization, to prevent the threat from destroying U.S. property with cyber, not kinetic, weapons.[147]

Justification of this proposed cyber ROE attribution solution comes from the standing international law of the sea and piracy.[148] If a pirated English vessel were to be sunk after firing on an American port, the English would not have any legal redress to the U.S. for the loss of that vessel.[149] Instead, it is understood that nation-states have a duty to prevent their vessels from being pirated and, if they fail in doing so, forfeit that vessel.[150] In fact, the U.N. Convention on the Laws of the Sea states that "any State having an opportunity [to take] measures against piracy, and neglecting to do so, would be failing in a duty laid upon it by international law."[151] Some scholars suggest that failing in that duty would not only mean the forfeiture of the destroyed vessel but also an additional legal claim for failing to prevent the piracy from occurring.[152] The justification given for policing piracy is the importance of the economic "choke point" areas in which pirate activities are largest.[153] Because high-volume international trade waters are economically important to nearly all of the nations of the world, a duty to prevent can exist.[154]

If vital shipping lanes are of such economic importance that a pirated ship could not only be fired upon without identifying its affiliation, but also force its formal owner to forfeit legal redress for its subsequent destruction, the world-wide-web is at least as equally important economically, and thus worthy of similar protection. Thus, just as there is a duty to prevent piracy, there must be a duty to prevent the "pirating" of computer systems. The proposed cyber ROE would allow a non-stun cyber-

---

[147] This lower level use of military force of course would only be able to stop the attack from continuing, not from bringing the person to justice. Author David Clark explains:

> To stop a DDoS attack, we want to shut off communication from the attacking machines, which would most obviously call for attribution at the level of an IP address. On the other hand, to bring the attacker—the bot master—to justice requires a different type of attribution—a person, not a machine.

David Clark, *Untangling Attribution*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS, *supra* note 111, at 26.

[148] *See* Duncan B. Hollis, *An E-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373, 412–13 (2011). Although the similarities between the sea and cyberspace are not discussed in this comment, some have made the argument that their similarities could lead to an extension of the law of the sea to cyberspace. *Id.*

[149] Eugene Kontorovich, *"A Guantánamo on the Sea": The Difficulty of Prosecuting Pirates and Terrorists*, 98 CALIF. L. REV. 243, 253 (2010).

[150] *Id.*

[151] *Id.* (quoting *Report of the International Law Commission to the General Assembly*, 11 GAOR Supp. (No. 9) at art. 38 cmt. 2, U.N. Doc. A/3159 (1956)).

[152] *Id.*

[153] Leticia M. Diaz & Barry Hart Dubner, *On the Evolution of the Law of International Sea Piracy: How Property Trumped Human Rights, the Environment and the Sovereign Rights of States in the Areas of the Creation and Enforcement of Jurisdiction*, 13 BARRY L. REV. 175, 182–83 (2009).

[154] *Id.* at 183.

weapon to be launched with only reasonable authorization. The proposed cyber ROE would put the world on notice that if they fail to prevent their systems from being used in coordinated attacks, they might lose it either temporary or permanently. This same duty to prevent computers from being pirated would apply to both foreign and domestic citizens who own personal computers.[155] Obviously, foreign countries would be upset if U.S. military forces damaged either their property or their civilian's property but, as stated by another scholar, "it seems unlikely that a nation would complain very loudly if its neighbor nation returned fire against a terrorist sniper firing from its territory."[156]

Professor Duncan Hollis of Temple University recently proposed a similar idea but suggested that the key to combating cyber-attacks is attributing attacks and taking drastic actions to stop those actors to deter others.[157] He suggested that if a country were being attacked, that country could send a cyber "SOS" to neighboring countries like a ship under fire would do in the ocean.[158] His proposal would thus extend a duty to respond to an "E-SOS" to neighboring countries.[159] However, his proposal seems to overlook the fact that cyber-attacks are likely to be so swift and so crippling that by the time a neighboring partner were to receive the message and attribute it, the attack would be over and any counter-attack would lack the necessity element, discussed above, to warrant a response, as there would no longer be a reason to have to launch an attack.[160] This comment's proposed cyber ROE offers a better approach by extending the piracy-like duty to prevent a computer from being taken in the first place.

The proposed cyber ROE duty-to-prevent standard was also recently used by the U.S. in the war on terror.[161] After 9/11, nation-states were warned that any nation that failed its duty to prevent terrorist attacks on other nations would have those acts imputed to them.[162] Thus, under this comment's proposed cyber ROE, if an attack is long in duration or causes severe physical destruction of U.S. property, the military could, with reasonable attribution, deploy more powerful cyber-weapons to stop the attack, regardless of whether or not the attack were ever completely attributed. This blanket exception would provide the possibility that the

---

[155] Sklerov, *supra* note 105, at 43–48. Of course, implementing such an idea would be difficult to do. *See*, *e.g.*, Susan Brenner, *Toward A Criminal Law for Cyberspace: A New Model of Law Enforcement*, 30 RUTGERS COMPUTER & TECH. L.J. 1 (2004).

[156] U.S. DEPT. OF DEFENSE, OFF. OF GEN. COUNS., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 22 (1999), http://au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf.

[157] Hollis, *supra* note 148, at 396.

[158] *Id.* at 408–09.

[159] *Id.*

[160] *See* discussion *supra* Part III.A.

[161] *See* Sklerov, *supra* note 105, at 44–48.

[162] *See id*. In the war on terror this U.S. position has successfully intimidated other countries into not harboring or aiding and abetting terrorists, given the fate that Afghanistan suffered for having done so.

U.S. could be unknowingly attacking another nation-state. However, as in the current state of international law towards piracy, those nation-states would have no redress, having failed in their duty to prevent the system from being overtaken. Any attacks could be countered with stun cyber-weapons without even reasonable attribution. Kinetic attacks with real-world weapons would have to be completely attributed.

4. Distinction

One final principle mandated by the laws of war is distinction.[163] Distinction under international law serves as a reminder to battlefield commanders that they must distinguish between civilian and military targets and that they must do all possible to minimize civilian casualties or property destruction in a military action.[164] Distinction has grown remarkably harder to implement because in modern warfare "a government [draws] upon national resources and mobilize[s] its entire society to gain total victory," civilians and their "place[] of work, railway lines, ports and . . . homes[]" are now used to prepare for and launch attacks, and could potentially become targets.[165] Thus, under this comment's proposed cyber ROE those targets which have a dual purpose, those that serve both a military and civilian use, can be targeted by military officials.[166] If the U.S. was being attacked by another nation-state or group in a large cyber onslaught, the military could conceivably attack the civilian power network, ISPs, or dual-use buildings, with either cyber, or if completely attributed and necessary to counter the hostile act, regular, kinetic weapons. However, because power plants and ISPs are extremely important to civilians and humanitarian organizations, authorization would have to be given before military leaders could target them with *any* cyber-weapons, including those that would only stun them, in order to ensure distinction is enforced. Finally, while power plants or ISPs could conceivably be considered a dual-use system, the proposed cyber ROE would not allow an attack on large banking websites unless they are state-run organizations.

Distinction poses another interesting problem with cyber-attacks since non-state actors can attack and civilian computers can be used against their will in coordinated attacks. Can the military attack the personal property of private citizens and observe distinction? The proposed cyber ROE would allow the military to attack non-state actors who "directly participate in hostilities" or who are members of a cyber-armed non-state

---

[163] U.N. Charter art. 51; Schaap, *supra* note 25, at 150.

[164] *See* Schaap, *supra* note 25, at 153–54.

[165] Paul Kennedy & George J. Andreopoulos, *The Laws of War: Some Concluding Reflections*, *in* THE LAWS OF WAR: CONSTRAINTS ON WARFARE IN THE WESTERN WORLD 214, 217 (Michael Howard et al. eds., 1994).

[166] Dunlap, *supra* note 52, at 89; Schaap, *supra* note 25, at 158–59.

actor group to be targeted by the military.[167] The proposed cyber ROE will remind commanders to limit civilian casualties, but would also allow the U.S., under some circumstances, to attack these "direct participants" who waive their civilian status by attacking.

But what if only the property of civilians is the direct participant in hostilities without the intent of their owners to participate? Can the military attack those targets? This comment's proposed cyber ROE would allow the military to use low-level stun weapons to disable those attacking systems. U.S. national security concerns must outweigh the concerns of private citizens who would be temporally prohibited from using their computers.

IV. CONCLUSION

Technology is constantly changing and the way in which people wage war is shifting. U.S. ROE must be clear and flexible to give commanders all that they need to protect the U.S. from incoming attacks. When targets of national security are targeted, it is the military, not local law enforcement, which must respond to the attack. Counter-attacks must be carefully calculated in order to meet international guidelines that regulate how war is to be conducted. The ROE proposed in this comment provide the needed flexibility while staying within established international rules. Obviously, more debate is needed on this issue, as well as the development of mission accomplishment rules; rules that would govern the use of cyber-weapons in a specific campaign or in conjunction with an offensive.

[167] Dunlap, *supra* note 52, at 90.