A Survey and Examination of the Adequacy of the Laws Related to Cyber Warfare

DONDI S. WEST*

This paper argues that the current rules of war can address the emerging issues raised by cyber warfare. The author begins by giving a survey of the laws that have the biggest impact on cyber warfare. Next, the author discusses several popular issues that may have unnecessarily intensified the cyber warfare debate. The author then asserts the following five reasons why the U.S. should not enter into an international treaty for cyber warfare: (1) combatant commanders already have proper guidelines for conducting cyber warfare; (2) fields of law are seldom demarcated by technology; (3) an unintended consequence of a cyber warfare law is that it may pose an undue limitation on a primarily non-lethal strategic deterrence; (4) our adversaries are unlikely to comply; and (5) the rate of technology growth will outpace the ability for an international cyber regime to produce responsive policy, while the flexibility allotted by the UN Charter and laws of war are able to absorb technological advances. The author concludes that the current UN Charter and Laws of War should continue to govern cyber warfare and that creating an international treaty or law for cyber warfare would do more harm than good and seriously cripple our ability to conduct war.

I. Introduction

Immediately upon taking office, and in the midst of the worst economic downturn since the Great Depression, President Barack Obama ordered a 60-day "clean-slate" study to review the plans, programs, and activities related to cyber security ("the 60-day Study").[1] Although many people did not expect President Obama to enter the White House with cyber security as a

* Dondi West is a Senior Cyber Intelligence and Policy Analyst at Booz Allen Hamilton and former U.S. Navy Information Warfare Officer. He holds a B.S. in Mathematics, a M.S. in Applied Information Technology, and a Juris Doctor degree from The University of Maryland School of Law, where he was an Editor of the *Maryland Law Review*. Dondi's scholarly interests include information operations and warfare policy, information privacy law, and cyberspace law.

[1] Siobhan Gorman, *Hathaway to Head Cybersecurity Post*, Wall St. J., Feb. 8, 2009, *available at* http://online.wsj.com/article/SB123412824916961127.html (last visited July 21, 2009).

main concern, an investigation of recent events shows why securing cyberspace is a major National Security priority of the Obama Administration.

During the Russia-Georgia conflict in August 2008, a multi-faceted cyber attack was conducted against the Georgian infrastructure and key government websites.[2] The attack modalities included defacing websites; web-based psychological operations; a fierce propaganda campaign; and distributed denial-of-service attacks.[3] The public witnessed one of the most vivid accounts of Cyber Warfare, when CNN's Wolf Blitzer attempted to interview Georgian President Mikhail Saakashvili by phone on his live news program during conflict. CNN couldn't reach President Saakashvili initially.[4] President Saakashvili blamed the difficulty connecting on a "cyber attack" against Georgia's telephone system. In addition to the situation described by President Saakashvili, attackers defaced the Georgian Ministry of Foreign Affairs' website with an image of Adolf Hitler next to an image of President Saakashvilli.[5]

Most recently, in April 2009, the Wall Street Journal ("WSJ") reported that cyber spies penetrated the US electrical grid.[6] Days later, on the front page, the WSJ reported that cyber hackers had breached the Pentagon's $300 billion Joint Strike Fighter project.[7] On July 4, 2009, cyber attackers disabled a number of US government websites, including the Treasury Department, Secret Service, Federal Trade Commission and Transportation Department sites.[8]

These incidents exemplify the scope of the risks posed by cyber security, and shows why the Obama Administration now consider securing cyberspace a vital National Security priority.

---

[2] Noah Shachtman, *Georgia Under Online Assault*, WIRED, Aug. 10, 2008, http://www.wired.com/dangerroom/2008/08/georgia-under-o/.
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] Siobhan Gorman, *Electricity Grid in U.S. Penetrated By Spies*, Wall St. J., Apr. 8, 2009 at A1.
[7] Siobhan Gorman, *Computer Spies Breach Fighter-Jet Project*, Wall St. J., Apr. 21, 2009 at A1.
[8] Kelly Olsen, *Massive Cyber Attack Knocked Out Government Web Sites Starting on July 4*, THE HUFFINGTON POST, Jul. 8, 2009, http://www.huffingtonpost.com/2009/07/07/massive-cyber-attack-knoc_n_227483.html.

In May of 2009, the White House released the results of its 60-day Study. The results included "near-term" and "mid-term" action plans, which together outlined 24 actions that should be taken to assist in putting the U.S. on course to secure cyberspace.[9] One of the near-term action items makes a recommendation to "[c]onvene appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the Federal government."[10] Although this action item recommends that legal analysis be conducted concerning "cybersecurity-related issues," it is rather broad and vague. In particular, the government is not required to address the unique legal issues that arise as a result of the U.S.

---

[9] The White House, *Cyberspace Policy Review*, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (last visited July 21, 2009). In particular, the action plan included the following steps:

1. Appoint a cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities; establish a strong NSC directorate, under the direction of the cybersecurity policy official dual-hatted to the NSC and the NEC, to coordinate interagency development of cybersecurity-related strategy and policy.
2. Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure. This strategy should include continued evaluation of CNCI activities and, where appropriate, build on its successes.
3. Designate cybersecurity as one of the President's key management priorities and establish performance metrics.
4. Designate a privacy and civil liberties official to the NSC cybersecurity directorate.
5. Convene appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the Federal government.
6. Initiate a national public awareness and education campaign to promote cybersecurity.
7. Develop U.S. Government positions for an international cybersecurity policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.
8. Prepare a cybersecurity incident response plan; initiate a dialog to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize their contribution and engagement.
9. In collaboration with other EOP entities, develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure; provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions.
10. Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation.

Id. at vi.

[10] *Id.*

conducting and defending against cyber warfare. In fact, legal scholars are involved in an intense debate on whether there should be a new set of laws written to govern cyber warfare.[11] Some legal scholars even advocate that there should be an international treaty for cyber warfare.

This article first surveys the current legal frameworks governing cyber warfare.[12] Next, it comments on several exaggerated hot-button issues.[13] It then argues that the traditional laws of war give combatant commanders the tools they need to conduct warfare in the information age.[14] Creating an international treaty for cyber warfare would do more harm than good.

II. Introduction to Computer Network Operations and the Actors Involved

Analysts often discuss the concepts of cyber warfare and cyber security in overly-broad terms. For example, if a cyber actor gains unauthorized access to a computer network and copies data, then a commentator may refer to this act as a "cyber attack."[15] But, if the cyber actor was merely snooping and didn't alter the performance or content of the network, then a cyber attack hasn't occurred sense military doctrine divides cyber acts into three separate domains collectively called Computer Network Operations.[16] According to Joint Publication 3-13, the full-spectrum of Computer Network Operations ("CNO") encompasses three domains: Computer Network Attack ("CNA"), Computer Network Exploitation ("CNE"), and Computer Network Defense ("CND").[17] Within the military domain, CNO is considered one of five core capabilities under Information Operations ("IO").[18] The other capabilities include Psychological

---

[11] *See infra* Part IV.
[12] *See infra* Part III.
[13] *See infra* Part IV.
[14] *See infa* Part V.
[15] *See e.g. supra* Note 6.
[16] JOINT CHIEFS OF STAFF, JOINT PUB. 3-13, INFORMATION OPERATIONS ix (February 13, 2006), *available at* http://tinyurl.com/d3dfsc.
[17] *See generally* JOINT CHIEFS OF STAFF, JOINT PUB. 3-13, INFORMATION OPERATIONS ix (February 13, 2006), *available at* http://tinyurl.com/d3dfsc.
[18] *Id.*

Operations[19] ("PSYOPS"), Military Deception[20] ("MILDEC"), Operations Security[21] ("OPSEC") and Electronic Warfare[22] ("EW"). Warfighters integrate these five IO capabilities to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.[23] The Joint Publication goes on to define each of the three domains of CNO. CNA includes actions taken via computer networks to disrupt, deny, degrade, or destroy the information within enemy computers and computer networks.[24] CND includes actions taken via computer networks to protect, monitor, analyze, detect and respond to network attacks, intrusions, disruptions or other unauthorized actions that would compromise or cripple defense information systems and networks.[25] CNE includes enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks.[26] Analyst and commentators tend to use the term "Cyber" in an overly broad manner, appending the term to virtually anything that is computer related. It is therefore necessary to understand Cyber within the context of which of the three CNO domains are being referenced. An example of CND would be deploying an intrusion detection system to protect a government network. An example of CNE would include gaining access to an adversary network's email server and analyzing email content for intelligence purposes.[27] Michael N. Schmitt, Stockton Chair at the Naval War College, gives an excellent description of CNA by describing several CNA scenarios:

---

[19] *See generally* JOINT CHIEFS OF STAFF, JOINT PUB. 3-53, JOINT DOCTRINE FOR PSYCHOLOGICAL OPERATIONS (September 5, 2003).
[20] *See generally* JOINT CHIEFS OF STAFF, JOINT PUB. 3-13.4, MILITARY DECEPTION (July 13, 2006).
[21] *See generally* JOINT CHIEFS OF STAFF, JOINT PUB. 3-13, INFORMATION OPERATIONS (February 13, 2006).
[22] *Id.*
[23] JOINT CHIEFS OF STAFF, JOINT PUB. 3-13, INFORMATION OPERATIONS ix (February 13, 2006), *available at* http://tinyurl.com/d3dfsc.
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] The "networking snooping" example given at the beginning of this paragraph is also an example of CNE.

Hypothetical examples of CNA, some realistic, others stretching credulity, abound in literature. Consider just a few.

> (1) Trains are misrouted and crash after the computer systems controlling them are maliciously manipulated.
>
> (2) An information blockade is mounted to limit the flow of electronic information into or out of a target state.
>
> (3) Banking computer systems are broken into and their databases corrupted.
>
> (4) An automated municipal traffic control system is compromised, thereby causing massive traffic jams and frustrating responses by emergency fire, medical, and law enforcement vehicles.
>
> (5) Intrusion into the computer system controlling water distribution allows the intruder to rapidly open and close valves. This creates a hammer effect that eventually causes widespread pipe ruptures.
>
> (6) A logic bomb set to activate upon initiation of mass casualty operations is imbedded in a municipal emergency response computer system.[28]

Although CND and CNE are unavoidable issues when it comes to Cyber Warfare, this article is primarily concerned with the laws related to CNA. Thus, the term Cyber Warfare, for the purposes of this article, is being referenced in the context of conducting or responding to a CNA on government computer systems or a nation's critical infrastructure. Governments use the term "critical infrastructure" to describe assets that are essential for the functioning of a society and economy.[29] For example, homeland security analysts consider the U.S. electrical grid to be critical infrastructure because a significant outage is capable of causing widespread damage to health, communication, economic, transportation, and other systems.[30] Thus, in addition to attacks on government systems, a cyber attack on a nation's critical infrastructure can also be considered a CNA.[31]

---

[28] Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 892-93 (1999).
[29] *See generally* John Moteff, CRITICAL INFRASTRUCTURE AND KEY ASSETS: DEFINITION AND IDENTIFICATION 1 (Congressional Research Service Report for Congress 2004) (2004).
[30] *Id.*
[31] *Id.*

Analyst must also make similar distinctions when considering the parties involved when a cyber act occurs. State actors, terrorist groups, criminals, or various other internet miscreants are all capable of conducting cyber attacks.[32] When one considers the notion of war, a conflict involving two or more nation states immediately comes to mind. A war, however, can also consist of a nation state and a non-state actor since "customary international law has evolved to allow states to apply the law of self-defense to non-state actors."[33] Such was the case when the UN Security Council passed UNSCR 1368, in support of OPERATION ENDURING FREEDOM, a day after the September 11, 2001 attacks on the Pentagon and World Trade Center ("9/11"). This resolution explicitly recognized the United States' inherent right of individual or collective self-defense pursuant to Article 51 of the UN Charter against the terrorist actors who perpetrated the 9/11 attacks.[34] The author, therefore, and for the purposes of this paper, is considering two conflict scenarios: a nation state against another nation state; and a nation state against a non-state actor. Both of these scenarios can be addressed under the UN Charter.[35] A cyber act that is criminal in nature is outside the scope of this paper, and would be addressed under appropriate international criminal laws; as is two non-state actors involved in a cyber conflict. Thus, this paper is not concerned with international cyber crimes such as internet scams. In addition, a scenario such as a private Chinese hacking group attacking the website of a private Russian hacking group is also outside the scope of this paper. Indeed, as it relates to cyber warfare, attribution is one of the biggest challenges, and one can imagine a situation where a nation conducts cyber activities under the guise of private independent hacking groups, or even while appearing to be another nation state. Although attribution is a significant challenge, the

[32] *See generally* JEFFREY CARR, INSIDE CYBER WARFARE 15-30 (Mike Loukides ed., O'Reilly Media 2010) (2009).
[33] *Id.* at 53.
[34] *Id.*
[35] *Id.*

author considers attribution to be a separate and unique issue, independent of whether the rules of war are adequate for addressing cyber warfare.

III. A Brief Overview of Cyber Warfare's Current Legal Framework

The two main questions facing military operations in cyberspace are: (1) which interstate activities in cyberspace constitute a threat or use of force under international law; and (2) when such a threat or use of force does constitute an armed attack under international law, how does that law of armed conflict apply to the lawful exercise of the inherent right of self-defense in cyberspace.[36] This section is, therefore, organized according to the following two regimes: Pre-Hostilities Law and Post-Hostilities Law; both in the context of CNAs.

*A. Pre-Hostilities Law (*Jus ad Bellum*): There is a general prohibition against all uses of force, except those sanctioned by the UN Security Council or done in self-defense.*

Jus ad bellum ("Right to wage war") has its foundations in the United Nations ("UN") Charter. The UN Charter mandates a general prohibition against the use of force, stating in article 2(4) that "[a]ll members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or any other manner inconsistent with the Purposes of the United Nations."[37] Commentators interpret Article 2(4) in two distinct ways. First, a minority of commentators interpret Article 2(4) as banning only the use of force directed at the territorial integrity or political independence of a state. Second, the majority of commentators believe that the minority's emphasis on territorial integrity and political independence are merely intensifiers, and that the article constitutes a general

[36] THOMAS C. WINGFIELD & JAMES B. MICHAEL, AN INTRODUCTION TO LEGAL ASPECTS OF OPERATIONS IN CYBERSPACE 10 (Naval Postgraduate School) (explaining that two important legal issues related to cyber warfare are (1) when does a CNA constitute a threat or use of force, and (2) how do the laws of armed conflict govern cyber warfare) (2004); *see also* JEFFREY CARR, INSIDE CYBER WARFARE 31-43 (Mike Loukides ed., O'Reilly Media 2010) (2009).

[37] U.N. CHARTER art. 2, para 4.

prohibition against all uses of forces, subject only to the exceptions stated in the UN Charter. The majority's interpretation is supported by the "or any other manner" language in Article 2(4), in that it can be argued that virtually any other use of force, not authorized by the Charter, is prohibited.[38] The majority's interpretation is also supported by the historic context in which the Charter was drafted; the preamble specifically states that "to save succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind" is a principal aim of the UN Charter. The majority's view is now considered to be a part of customary international law, which, therefore, bans the use of armed force except for two situations authorized by the UN Charter.

First, Chapter VII, entitled "Action With Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression," gives the UN Security Council the authority to "determine the existence of any threat to the peace, breach of the peace, or act of aggression" and to take military and nonmilitary action to "restore international peace and security." In this case, and pursuant to Article 39, the Security Council must first determine whether a threat to peace, a breach of peace or an act of aggression exists. Based upon this determination, the Security Council then has the power under Article 41 to employ measures short of force, including a wide variety of diplomatic and economic sanctions against the target State, to compel compliance with its decisions. Should those measures prove inadequate, the Security Council has the power to authorize member States to employ military force in accordance with Article 42.

[38] *Id.*

Second, Article 51 of the UN Charter provides for the right of countries to engage in military action in self-defense, including collective self-defense.[39] Article 51 of the Charter provides:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

The inherent right of self-defense has been manifested in three recurring areas: (1) protection of nationals and their property located abroad; (2) protection of a nation's political independence; and (3) protection of a nation's territorial integrity. In all acts of self-defense, the UN Charter requires the act to be necessary,[40] proportional,[41] and timely.[42] Thus, a government, pursuant to its right of self-defense, may conceivably respond to a distributed denial of service (DDoS) attack,[43] with a computer attack of its own. Here, the aggrieved government would be justified

---

[39] *See* INTERNATIONAL AND OPERATIONAL LAW DEPARTMENT, OPERATIONAL LAW HANDBOOK 1-3 (Marie Anderson & Emily Zukauskas eds., The Judge Advocate General's Legal Center & School, U.S. Army)(2008).

[40] Here, one must consider the exhaustion or ineffectiveness of peaceful means of resolution, the nature of coercion applied by the aggressor State, objectives of each party, and the likelihood of effective community intervention.

[41] Here, the actor must limit force in magnitude, scope, and duration to that which is reasonably necessary to counter a threat or attack.

[42] A delay of a response to an attack or threat of attack attenuates the immediacy of the threat and the necessity to use force in self-defense.

[43] A distributed denial of service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to legitimate users. WEBOPEDIA http://www.webopedia.com/TERM/D/DDoS_attack.html.

in attacking the computer systems where the DDoS originated (the "originating computers").[44] Thus, the aggrieved government would have shown that its act of self-defense was: (1) "necessary" to prevent the originating computers from attacking it again; (2) "proportional" because it essentially responded in kind with a computer attack of its own; and (3) timely because the act of self-defense was done in a reasonable time following the original attack.

*B. Post-Hostilities Law (*Jus in Bello*): When deciding if a target can be attacked, a combatant commander must consider distinction; balancing military necessity with humanity; and proportionality*

Once two nations are in armed conflict with each other, the law of war applies.[45] The Department of Defense (DoD) mandates the law of war to apply in *all operations* including military operations other than war (emphasis added).[46] Thus, combatant commanders must adhere to the law of war during Cyber operations.[47]

Commanders may only attack lawful military targets. Lawful military targets are "combatants and those objects, which, by their nature, location, purpose, or use, effectively contribute to the enemy's war-fighting or war-sustaining capability and whose total or partial destruction, capture, or neutralization would constitute a definite military advantage to the attacker under the circumstances at the time of the attack."[48] "[T]argets of the enemy that indirectly but effectively support and sustain the enemy's war-fighting capability may also be

---

[44] Here, the problem of attribution arises again. Although difficult, there are methods for locating the originator of a DDoS attack. *See e.g.* IHAB HAMADEH, ATTACK ATTRIBUTION FOR DISTRIBUTED DENIAL-OF-SERVICE AND WORM ATTACKS (Pennsylvania State University 2006) (2006).
[45] *See* Condition (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, art. 2 (stating that the law of war comes into play during international armed conflict).
[46] *See* DoDD 5100.77, The Law of War Program.
[47] Here, the author is defining "combatant commander" as the commander of a combat unit or brigade, who has the authority to decide which targets should be attacked.
[48] Additional Protocol I to the Geneva Conventions art. 52.

attacked."[49] A combatant commander must consider three factors when deciding if a target can be attacked:

(1) Distinction

(2) Balancing Military Necessity with Humanity

(3) Proportionality[50]

1. Distinction

Two concepts emerge under the principle of distinction: (1) that there be a formal distinction between combatant and noncombatant persons;[51] and (2) the duty to conduct warfare in a manner that minimizes harm to civilians and other noncombatants. Because this paper is primarily concerned with the act and not the actor of cyber warfare, an emphasis is placed on the latter concept of distinction. However, as a note, lawful combatants include the uniformed regular armed forces of a state, who have the sole right to participate in armed attacks or hostilities against an enemy.[52]

A combatant commander is required to distinguish between military and civilian objects, as the central idea of distinction is that only valid military targets should be attacked. Protocol Additional to the Geneva Conventions[53] covers distinction in this respect. The general rule for distinction is embodied in Article 48, which states that "[i]n order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects

[49] *Id.*
[50] *See* U.S. Dep't of the Navy, NWP 1-14M, Commander's Handbook on the Law of Naval Operations (Jul. 2007).
[51] 1949 Geneva Convention (III) Relative to the Treatment of Prisoners of War ("GPW"), art. 4.
[52] *Id.*
[53] The full name is Protocol Additional to the Geneva Conventions of 1949, and Relating to the Protection of Victims of International Armed Conflict ("GPI").

and military objectives and accordingly shall direct their operations only against military objectives." Article 50 defines who is a civilian and what is a civilian population. Article 51 describes the protection that should be given to civilian populations. Article 52 regulates the targeting of civilian objects. Article 57 outlines specific steps that a commander must take in order to verify that and object is not civilian in nature.

Drawing the line of distinction is not easy. Complicating the matter for commanders, civilian objects can temporarily become valid military objectives based on location, purpose, or use.[54] Major Eric Talbot Jensen, a Professor in The International and Operational Law Department at The U.S. Army's Judge Advocate General School, explained the concept of dual use objects using an infamous bridge example:

> [A] bridge that normally carries civilian traffic and would be considered a civilian object would become a military objective based on its location if it became the means for the enemy's armed forces to move to the battle. While still serving as a primary means for civilian transport over the river, the bridge is now a military object, as it is the primary means for the military to cross that same river. Objects like this are known as dual-use objects; objects that simultaneously serve civilian and military objectives. These dual-use objects present a unique challenge for commanders.[55]

It is important to note that even when engaging a dual-use object found to be a military objective, the commander, when possible, must make an effort to limit his attack to the portions

---

[54] *See* GPI, *supra* note 21, art. 57, para. 2(a)(ii), 1125 U.N.T.S. at 29.
[55] Major Eric Jensen, *Unexpected Consequences From Knock-On Effects: A Different Standard for Computer Network Operations?*, 18 AM. U. INT'L L. REV. 1145, 1156-57 (2003).

of the dual-use object that is military in nature. Furthermore, once the dual-use object ceases to support military objectives, it must be looked upon as being civilian in nature.[56]

Distinction comes into play in attacks upon an enemy's computer network. Because of the interconnective nature of the internet, that network would likely be dual use, as civilian internet service providers enable online networks, while supporting the enemy's military objective of communicating. As discussed above, a combatant commander would need to take reasonable steps to limit the attack to the portion of the network used by the enemy. If the combatant commander releases a computer virus that propagates randomly through networks on which essential civilian functions reside, such as banking, medical care or electrical power, then the principle of distinction would likely be violated.

2. Balancing Military Necessity with Humanity

In addition to distinction, the combatant commander will have to balance military necessity with humanitarian principles. Under military necessity, an attack on a particular target must further a legitimate military objective or confer a definite military advantage.[57] Although the principle of military necessity appears to be a liberal one, it is not unchecked. It must be balanced against the principle of humanity.[58] That is, an attack should not cause unnecessary suffering or superfluous injury in order to accomplish a military purpose.[59]

An example of military necessity being balanced with humanity, in the cyber context, can be based on the fictitious attack on an enemy's computer system that controls the enemy's power supply. Most power grids are controlled and monitored by supervisory control and data

---

[56] *Id.*
[57] Protocol 1 to the Geneva Conventions art. 52(2).
[58] *See* Hague Convention on Land Warfare art. 22 (1907) (demonstrating the essential relationship between military necessity and humanity).
[59] *See* GPI art. 35 para. 2.

acquisition ("SCADA") systems. Because SCADA systems are types of computer information systems, they are vulnerable to CNA. A combatant commander may, therefore, decide to attack a SCADA system, prior to a ground assault, in order to sabotage the enemy's warfighting capability. Although disabling the power supply might be a legitimate military objective, the commander must weigh this objective against humanitarian gains and losses such as extensive power loss, or power loss to a civilian hospital or other critical civilian objects. Using the principle of humanity, targets that might be deemed critical civilian infrastructures, are protected under established valid military objectives. The decision to attack critical civilian infrastructures, which may be a dual-use target, must be weighed against the principle of humanity prior to any engagement decisions. As a note, the combatant commander is only required to weigh military necessity against humanity. Taking the above example into consideration, a combatant commander can legally attack an enemy's power system, despite its affect on a civilian hospital, if the situation warrants it. For example, a combatant commander is likely not in violation of this principle, if he decided to disable the enemy's power supply, after learning that doing so would enable the capture or kill of a high value target like Osama Bin Laden. Although this is an unlikely scenario, it shows that this principle is essentially a judgment call that the combatant commander must make.

3. Proportionality

A simple way to remember the principle of proportionality is by recalling the popular phrase that 'the ends must justify the means.' In other words, the incidental harm caused to civilians or civilian property must be proportional and not excessive in relation to the concrete and direct military advantage anticipated by an attack on a military objective.[60] Taking the

[60] Yoram Dinstein, *The Conduct of Hostilities Under the Law of International Conflict* 12-23 (2004).

above requirement to balance military necessity and humanity into consideration, proportionality would be the tool by which they are balanced. The combatant commander ordering the attack is responsible for making the proportionality judgment. A corollary of the principle of proportionality is that the attacker has a responsibility to take reasonable steps to find out what collateral damage a contemplated attack may cause.[61] Applying proportionality in the context of a power supply scenario, one can see that proportionality is the calculus applied to determine whether the benefits from achieving the military objectives outweigh its negative collateral effects such as extensive power loss to the civilian population.

Once hostilities have begun, it is important to remember that a combatant commander must consider three factors when deciding if a target can be attacked: Distinction; Balancing Military Necessity with Humanity; and Proportionality. As discussed *infra* it is important to realize how these three principles apply to acts of Cyber Warfare.

IV. Well-Known and Often-Discussed Cyber Warfare Issues

The media, academic, military, and technology communities give vast attention to the topic of cyber warfare. Although much scrutiny has been given to the current laws of cyber warfare, the majority of criticisms argue that the current legal framework cannot address warfighting in cyberspace. Many people believe that the traditional laws of war are inadequate and should be rewritten. Others believe that nations should enter into an international treaty for fighting cyber warfare. This paper argues that the traditional laws of war can aptly guide nations in conducting and defending against cyber warfare. Before doing so, I provide commentary on three well-known issues that are often discussed in the cyber warfare community. First, the "use of force" debate is described. Second, the popular, but inaccurate "cyber arms race" analogy is

[61] *Id.*

discussed. Third, proposals for the creation of an international treaty for cyber warfare are explained.

A. The "Use of Force" Debate

As it relates to Cyber Warfare, a primary concern of *jus ad bellum* is whether a particular action of CNA equates to a "use of force" or "armed attack" under UN Articles 2(4), 39, or 51.[62] Based on these three UN Articles, the legality of a pre-hostility action depends on where that action falls along an imaginary spectrum of force.[63] This imaginary spectrum includes three zones: (1) below the threshold of a use of force under Article 2(4); (2) a use of force under Article 2(4) but shy of an armed attack under Article 51; or (3) an armed attack under Article 51 giving the victim state the right to respond to self-defense. Although "use of force" is commonly understood to consist of a kinetic military attack, such as an air strike, Article 2(4) also applies to "physical force of a non-military nature committed by any state agency."[64]

Scholars contend that determining when a particular act of CNA constitutes a use of force or an armed attack is difficult. "The dilemma lies in the fact that CNA spans the spectrum of consequentiality. Its effects freely range from mere inconvenience (e.g., shutting down an academic network temporarily) to physical destruction (e.g., as in creating a hammering phenomenon in oil pipelines so as to cause them to burst) to death (e.g., shutting down power to a hospital with no back-up generators)."[65] Because of this perceived dilemma, Schmitt proposed seven factors to determine whether a particular act of CNA amounts to a use of force under the

---

[62] *See generally* THOMAS C. WINGFIELD, THE LAW OF INFORMATION CONFLICT Part II (2000).
[63] *Id.* at 128.
[64] W.G. Sharp, *Critical Infrastructure Protections: A New Era of National Security*, 12 THE FEDERALIST SOC'Y INT'L AND NAT'L SECURITY L. NEWS 1, 1 (1998).
[65] Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 912 (1999).

UN charter.[66] To analyze a CNA issue *jus ad bellum*, Schmitt recommends applying a consequence based analysis using the following factors: (1) Severity; (2) Immediacy; (3) Directness; (4) Invasiveness; (5) Measurability; (6) Presumptive Legitimacy; and (7) Responsibility. Here, Professor Schmitt attempts to provide a multi-factor approach for determining whether a CNA amounts to an armed attack, explaining that:

> First, a cyber attack is an armed attack justifying a forceful response in self-defense if it causes physical damage or human injury or is part of a larger operation that constitutes an armed attack. Second, self-defense is justified when a cyber attack us an irrevocable step in an imminent (near-term) and unavoidable attack (preparing the battlefield). Finally, a State may react defensively during the last possible window of opportunity available to effectively counter an armed attack when no reasonable doubt exists that the attack is forthcoming.[67]

Although Schmitt's proposes a multi-factor test to determine when an act of CNA equates to a "use of force," at the onset, and as discussed *supra,* it is important to consider that the UN Security Council, prior to the commencement of hostilities, generally prohibits uses of force except for the two situations authorized by the UN Charter.[68] First, the Security Council has the sole authority and discretion to ratify (or sanction) any use of force; to include a very mild cyber attack.[69] Here, the author highlights the potential ratification or sanctioning of a "mild" cyber attack to emphasize the UN Council's broad authority; a cyber attack need not be

---

[66] Michael N. Schmitt, *The Sixteenth Waldemar A. Solf Lecture on International Law*, 176 Mil. L. Rev. 364, 417 (2003); Schmitt, *supra* note 28 at 914-15.
[67] *Id.* Similar to Schmitt's analysis, Thomas Wingfield also suggests a multi-factor approach to determine whether a CNA amounts to an armed attack. Arguing that "an armed attack may occur when a use of force or an activity not traditionally considered an armed attack is used in such a way that it becomes tantamount in effect to an armed attack." Wingfield proposes three factors to consider when looking at whether an activity is tantamount to an armed attack: scope; duration; and intensity. WINGFIELD, *supra* note 62, at 113.
[68] *See supra* Part III.A.
[69] *See supra* Part III.A.

of epic proportions to fall under the purview of the UN Council. For example, if China defaced a United States Government website, which is arguably a mild act, and likely wouldn't amount to a use of force under Schmitt's analysis, then the UN Council has the power to ratify or sanction that act. "The U.N. General Assembly defined aggression to include the use of 'any weapons' against another state. The use of such a clearly broad term as 'any' logically implies that the use of even minor weapons against a state could be considered an act of aggression, if the circumstances are of "sufficient gravity."[70] Thus, although unlikely, if a nation state sanctions the throwing of a stone towards another nation's embassy, then that mild act could be considered a use of force. This general prohibition also applies to the use of cyber weapons. Because the UN Charter generally forbids all uses of force, there is no need to engage in a multi-factor analysis. Second, Article 51 of the UN Charter provides for the right of countries to engage in military action in self defense, including collective self-defense.[71] Taking these two exceptions into consideration, it follows that a CNA equates to a use of force if and whenever the UN Council says so. If the UN Council determines that a CNA is a use of force, then the UN Council has the discretion to ratify or sanction it.[72] Said differently, anytime a nation state chooses to conduct CNA, that nation is taking a risk that the UN Council may sanction the act, because a use of force is assumed to be prohibited. In addition, a country is allowed to engage in CNA or use force, if the CNA is a recognizable act of self-defense.[73] Similar to the authorities granted pursuant to Articles 39 and 41, the UN Council has the authority to determine whether an act of self defense is a reasonable one. *Thus, a nation conducting any CNA, prior to hostilities, is legally doing so only in the case of reasonable self-defense; if self-defense is not*

[70] Major Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric* Definition, 64 A.F.L. REV. 65, 84 (2009).
[71] *See supra* Part III.A.
[72] *See supra* Part III.A.
[73] *See infra* Part III.A.

involved, then the nation actor is conducting CNA with the risk of being sanctioned by the UN Council. This may imply that the UN Council needs to implement means of monitoring all state-sponsored acts of CNA and become more aggressive in holding countries accountable for cyber acts, which is a challenge in and of itself, but it does not imply that the international laws of war are inadequate.

One may consider whether the UN Council should then adopt a uniform multi-factor test when reviewing cyber acts, similar to the test proposed by Schmitt. This framework would give the UN Council a set of factors for deciding whether to ratify or sanction a particular CNA. The dynamic nature of cyber warfare and the rate of technology advancement makes a "multi-factor test" a horrible candidate for a single and dispositive test for determining the legitimacy of a CNA. Professor Barton Beebe of the Benjamin N. Cardozo School of Law gives a stunning critique of legal multi-factor tests.[74] Beebe argues that although no particular factor is said to be dispositive in most multi-factor tests, in practice "judges employ 'fast and frugal' heuristics to short-circuit the multifactor analysis. . . [and that] [a] few factors prove to be decisive; the rest are at best redundant and at worst irrelevant."[75] Although Beebe's gives a general critique to multi-factor tests, his arguments are more relevant in the context of cyber warfare. With the dynamic nature of cyber warfare, and in light of the above criticism, a multi-factor test would be highly restrictive and should not be used as the one and only standard to assess the legitimacy of a CNA. The UN Council should maintain its broad authority to ratify or sanction acts of CNA, while using whatever methodology to do so as the situation warrants. Those who promote this issue as a major debate are misconstruing the UN's broad authority, ignoring the general

[74] Barton Beebe, *An Empirical Study of the Multifactor Tests for Trademark Infringement*, 94 CAL. L. REV. 1581, 1581 (2006).
[75] *Id.*

prohibition against all uses of force, and therefore, mistakenly concluding that international law is silent on the issue.

B. The Misleading Cyber Arms Race Analogy

Some analysts believe that the U.S., China, Russia and others are locked in a "Cyber Arms Race," reminiscent of the Nuclear Arms Race between the U.S. and Russia that became known as The Cold War.[76] In fact, a recent *Defense Tech* article goes so far as to make a direct comparison of the current cyber climate to the Cold War:

> A 'dead heat' is a race, campaign or other contest that is so close that it is impossible to predict the winner. That's what it looks like when it comes to the continuing race for cyber warfare supremacy, and experts agree this will be the case for the foreseeable future. With images of the Cold War and its associated arms race, as cyber warfare, cyber espionage, cyber attacks and cyber terrorism continues to evolve the top three leaders (US, Russia and China) are jockeying for position. [77]

Although the notion of a Cyber Arms Race makes a great cover story, this comparison is simply misleading.[78] It is a direct attempt to compare military cyber capabilities to nuclear weapons, and uses this comparison to give the exaggerated perception that some grave and imminent cyber danger exists that can only be prevented with the creation of "international cyber treaties;" similar to today's current Nuclear Treaties.

---

[76] *See e.g.* Jack Goldsmith, *Can we stop the global cyber arms race?*, N.Y. TIMES, Feb. 1, 2010, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/01/31/AR2010013101834.html.
[77] Kevin Coleman, *The Neck and Neck Cyber Arms Race*, DEFENSE TECH, Mar. 17, 2009, *available at* http://defensetech.org/2009/03/17/the-neck-and-neck-cyber-arms-race/.
[78] *See generally* Evgeny Morozov, *Cyber-Scare: The Exaggerated Fears Over Digital Warfare*, BOSTON REVIEW, July/August 2009, *available at* http://bostonreview.net/BR34.4/morozov.php.

C. Proposals for International Treaty for Cyber War.

Legal scholars have criticized the law of war as outdated as it relates to cyber warfare, and therefore call for the creation of an International Treatise for Cyber Warfare.[79] For example, Davis Brown suggests that applying the current law of war to cyber and information warfare "erroneously assumes that warfare by computer is not significantly different from warfare with kinetic weapons such as bombs and bullets."[80] Brown goes on to caution against assuming that conventional law of war "will resolve all of the new issues raised by the use of malicious code, denial-of-service attacks, and control of vital systems when used against the enemy." To support the above contention, Brown points out two paradigms that have emerged due to cyber and information warfare. First, that there is a shift in favored weaponry from kinetic weapons towards information weapons. Second, that there is a growing dependency on civilians and civilian objects when conducting warfare. Based on those two paradigms, Brown concludes that "[t]he square peg of conventional [law of war] does not fit neatly into the round hole of [cyber and] information warfare," and he therefore proposes an "International Convention To Regulate the Use of Information Systems in Armed Conflict." Brown goes on to state that this proposed body of law governing Cyber Warfare should be based on the current law of war, including the principles of Part III above, but not so much that the essence of Cyber and Information Warfare is crippled. Following the conclusion, Brown presents a Draft Convention Regulating the Use of Information Systems in Armed Conflict (the "Draft Convention").[81] In the Draft Convention, Brown fails to propose anything new under the current rules of war. For example, in Article 1,

---

[79] *See generally* Agence France-Presse, *UN Agency Calls for Global Cyberwarfare Treaty, 'driver's license' for Web Users*, THE RAW STORY, Jan. 30, 2010 *available at* http://rawstory.com/2010/01/agency-calls-global-cyberwarfare-treaty-drivers-license-web-users/.

[80] 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, 179-83 (2006).

[81] *Id.* at 215.

Brown defines several terms, which are already well-defined in the international, technology, and cyber warfare communities. In Article 3, Brown simply proposes that the current law of war be applied to information systems, stating that "[a]n act that violates the law of armed conflict if carried out by conventional means also violates the law of armed conflict if carried out by an information attack. An attack that does not violate the law of armed conflict if carried out by conventional means also does not violate the law of armed conflict if carried out using information systems."[82] Articles 4-17 merely implements the principles of distinction, balancing military necessity with humanity, and proportionality discussed *supra*. The remainder of the Draft Convention goes on to specify how the rules of warfare should be implemented in the context of cyber warfare. Brown, in the Draft Convention, failed to present any novel laws; he simply took the current rules of war and demonstrated how they already apply to cyber warfare.

V. Arguments Against Creating a Distinct Body of and International Treaty for Cyber Warfare Law.

Major Eric Jensen contends that the traditional laws of war actually compliment a commander's ability to conduct Cyber Warfare.[83] Jensen argues that the law of war accommodates a commander's use of CNA in that the commander only needs to determine "if, in good faith, he believes that the damage to civilian objects, and injury to civilians that is expected from the attack, given the circumstances as known to him at the time . . . is not excessive to the concrete and direct military advantage anticipated."[84] Jensen concludes that "the legal standard

[82] *Id.*
[83] *Jensen supra* note 55 at 1146-75.
[84] *Id.*

when considering potential unexpected consequences is no different in CNO than in normal kinetic operations and presents no significant addition to the standard targeting analysis."[85]

In addition to the reasons cited by Major Jensen, this paper also asserts that the traditional laws of war are able to handle the unique issues that arise as a result of conducting cyber warfare. The current UN Charter and Laws of War should, therefore, continue to govern cyber warfare. In fact, creating an international treaty or law for cyber warfare would do more harm than good and seriously cripple our ability to conduct war.[86] In particular, the U.S. should not support an international treaty or law for cyber warfare because: (1) combatant commanders already have proper guidelines for conducting warfare; even in the information age;[87] (2) fields of law are seldom demarcated by technology; (3) an unintended consequence of a cyber warfare law is that it may pose an undue limitation on a primarily non-lethal strategic deterrence; (4) our adversaries are unlikely to comply; and (5) the rate of technology growth will outpace the ability for an international cyber regime to produce responsive policy, while the flexibility allotted by the UN Charter and laws of war are able to absorb technological advances.

A. Fields of Law are Seldom Demarcated by Technology

Joseph Sommer argued against the creation of a distinct body of "Cyberlaw," asserting that: (1) cyberlaw is not a body of law in and of itself as technologies generally do not define bodies of law, (2) it is dangerous to consider Cyberlaw as its own body of law and that to do so will lead to the development of bad law, and (3) most legal issues posed by these technologies are not new at all and that existing law is flexible enough to deal with such issues. In doing so, Sommer highlights the facts that there was never a law of the steam engine despite its role in

---

[85] *Id.*
[86] *See e.g. infra* Part V.C.
[87] *See supra* Part III; *see also supra* Part IV.A.

society, nor is there really a law of the car today. Sommer concludes that the new informatics technologies do not support any discrete body of social practice, and therefore, Cyberlaw will not survive any longer than "the law of the Telephone" or "Space Law."[88] Although this argument has failed to gain traction in mainstream society, due to the fact that technology has driven changes in several areas of the law, Sommers' argument directly lends itself to the debate on the limited issue of whether there should be an international treaty or distinct body of cyber warfare law.[89] Similar to Sommers' argument, as it relates to warfare, there was not a law created for semi-automatic rifles or tanks, which were arguably more revolutionary to warfare than the computer. This is the exact reason why the Hague Rules of Aerial Warfare, crafted in the aftermath of the first use of aircraft in armed conflict, is a dead letter.[90] Similarly, other treaties were created due to hype instead of necessity, such as the treaty banning the use of environmental modification techniques in warfare,[91] the protocol banning weapons whose fragments cannot be detected by X-ray,[92] and the protocol banning the use of blinding lasers.[93] In each of the above situations, there was a new and exciting technology, and in a knee-jerk reaction, the international community responded with an unnecessary treaty. As it relates to cyber warfare, the lessons of the past must be considered. Furthermore, as shown *supra*, the current laws of war adequately addresses cyber warfare.[94] For example, prior to armed conflict,

---

[88] *See generally* Joseph Sommer, *Against Cyberlaw*, 15 BERK. TECH. L.J. 1145, 1145 (2000).
[89] *Id.*
[90] Hague Rules of Aerial Warfare, Feb. 19, 1923, 32 AM. J. INT'L L. SUPP. 12 (1938) (not in force).
[91] Convention on the Prohibition of Military or Any Hostile Use of Environmental Modification Techniques, May 18, 1977, 31 U.S.T. 333, 16 I.L.M. 88 (1977).
[92] Protocol I on Non-Detectable Fragments, annexed to Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects, Oct. 10, 1980, U.N. Doc. A/CONE95/15 (1980), 19 I.L.M. 1523, 1529 (1980).
[93] Protocol IV on Blinding Laser Weapons, annexed to Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects, Oct. 13, 1995, 35 I.L.M. 1206, 1218 (1996)
[94] *See supra* Part III.

there is a general prohibition against uses of force,[95] and during armed conflict, the principles of distinction, balancing military necessity with humanity, and proportionality must with be used.[96] Therefore, the current rules of war, prior to, and during hostility, encompass cyber warfare. In light of past lessons learned, and the fact that the current rules of war adequately addresses cyber warfare, the advent of cyber weapons or capabilities should not cause the warfare laws to be rewritten.

B. Undue Limitations on a Primarily Non-Lethal Strategic Deterrence

A strategic deterrence is generally defined as the actions of a state or group of states to dissuade a potential adversary from initiating an attack or conflict by the threat of retaliation by credibly demonstrating to an adversary that the costs of an attack would be too great and would outweigh any potential gains.[97] A popular example of a strategic deterrence is the mutually assured nuclear destruction that would occur should two opposing sides deploy a nuclear weapon; each opposing side is, therefore "deterred" from using their nuclear weapon.[98] Although cyber capabilities are unlikely to cause the same amount of devastation as nuclear weapons, they commonly serve as deterrents. For example, one nation state may not conduct a cyber attack due to the possibility of mutual destruction that may occur if the aggrieved nation responds with a cyber attack of its own.

An unintended consequence of a Cyber Warfare treaty is that it may pose an undue limitation on a primarily non-lethal strategic deterrence. Despite the many doomsday scenarios such as a nuclear power plant being hacked and causing a nuclear explosion, a "Cyber-Katrina"

---

[95] *See supra* Part III.A.
[96] *See supra* Part III.B.
[97] Col. Alan J. Parrington, *Mutual Assured Destruction: Mutually Assured Destruction Revisited, Strategic Doctrine in Question*, AIRPOWER JOURNAL, Winter 1997.
[98] *Id.*

is unlikely.[99] In fact, cyber warfare is unlikely to cause the loss of human life. It can be argued that cyber warfare is a primarily non-lethal strategic deterrence.[100] For example, "China's interest in achieving military effects via cyber warfare begins with deterrence. The goal is not to deter other nations from conducting cyber warfare against the PRC; rather, it is to use the threat of cyber warfare to deter an actor from behaving in a manner that is in opposition to Chinese strategic interests."[101] To this day, no human being has died as a result of a cyber attack.[102] Although cyber warfare is primarily non-lethal, a CNA is capable of causing physical harm. One can imagine such scenarios such as a CNA causing airplane crashes, due to cyber attacks on air traffic control systems, or a nuclear explosion, due to cyber attacks on a nuclear power plant's SCADA system. However, these scenarios are unlikely.[103] Furthermore, as discussed *supra*, these acts would likely violate the current rules of war.[104] Because cyber warfare is primarily non-lethal, and due to its deterrence capability, it may be the greater of two evils when it is compared to traditional kinetic weaponry such as missiles. In light of the UN Charter's guiding principle of preserving human life, proponents of the creation of a cyber warfare treaty should consider the fact that such a treaty may have the effect of limiting a primarily non-lethal weapon, and possibly shift the weaponry trend back to the use of kinetic weapons.

C. Our Real Adversaries are Unlikely to Comply with a Cyber Treaty

Our adversaries are primarily non-state sponsored. In fact, the phrase "War on Terror" was used to denote a global military, political, legal and ideological struggle against

---

[99] *See* Evgeny Morozov, *Cyber-Scare: The Exaggerated Fears Over Digital Warfare*, BOSTON REVIEW, July/August 2009, *available at* http://bostonreview.net/BR34.4/morozov.php.
[100] *Id.*
[101] Brian M. Mazanec, *The Art of (Cyber) War*, The Journal of International Security Affairs, Spring 2009—Number 16 (2009) *available at* http://www.securityaffairs.org/issues/2009/16/mazanec.php.
[102] *Id.*
[103] *See* Evgeny Morozov, *Cyber-Scare: The Exaggerated Fears Over Digital Warfare*, BOSTON REVIEW, July/August 2009, *available at* http://bostonreview.net/BR34.4/morozov.php.
[104] *See supra* Part III.

organizations designated as terrorist and regimes that were accused of having a connection to them, with a particular focus on militant Islamists and al-Qaeda. A terrorist organization like Al'Qaeda is unlikely to comply with any cyber treaty. Creating an international law will, therefore, have the actual effect of crippling our warfighting ability, while our real adversaries continue to run rogue. In addition, even in the event of us encountering a state-sponsored adversary, attributing cyber attacks to a particular entity is difficult. "The challenge of attribution in cyberspace provides China [and others] with plausible deniability and makes cyber warfare all the more attractive. "Independent" patriotic hackers, cultivated and loosely controlled as a 21st-century version of Mao's "People's War," provide the perfect mechanism to give the PRC cyber threat credibility."[105] If we were to enter into a cyber warfare treaty, we would essentially be volunteering to fight war "with one hand behind our back," while those we are likely to fight against will do so with no rule of law in mind—let alone a rule governing cyber warfare.

D. The rate of technology will outpace the ability for an international cyber regime to produce responsive policy, while the flexibility allotted by the UN Charter are able to absorb technological advances.

An analysis of the history of technology shows that technological change is exponential, contrary to the common-sense "intuitive linear" view. So we won't experience 100 years of progress in the 21st century -- it will be more like 20,000 years of progress (at today's

[105] Brian M. Mazanec, *The Art of (Cyber) War*, The Journal of International Security Affairs, Spring 2009—Number 16 (2009) *available at* http://www.securityaffairs.org/issues/2009/16/mazanec.php.

rate). The "returns," such as chip speed and cost-effectiveness, also increase exponentially. There's even exponential growth in the rate of exponential growth.[106]

In the time it will take the international community to produce cyber policy, technology would have gone through another revolution.[107] Furthermore, if we produce a legal framework solely based on cyber warfare, then hackers will be smart enough to find loopholes in the law and craft their cyber attacks around those laws. Instead, we should allow the continued flexibility of the UN Charter and laws of war to continue to govern the way we conduct warfare; even in the information age. This is exactly why the UN Charter is broad and does not limit itself to any particular technology.

VI. Conclusion

The laws of war will be tested by cyber warfare in two situations: first, prior to the commencement of an armed conflict;[108] second, when an armed conflict is ongoing.[109] In each of these situations, the current laws of war can address the emerging issues raised by cyber warfare. Although several hot-button issues related to cyber warfare are often discussed and fuel the cyber warfare debate, they may not be issues at all.[110] A careful analysis shows that the current UN Charter and Laws of War should continue to govern cyber warfare. Creating an international treaty or law for cyber warfare would do more harm than good and seriously cripple our ability to conduct war.[111]

---

[106] Ray Kurzweil, *The Law of Accelerating Returns*, KurzweilAI.net, Mar. 7, 2010 *available at* http://www.kurzweilai.net/articles/art0134.html?printable=1.
[107] *Id.*
[108] *See supra* Part III.A.
[109] *See infra* Part III.B.
[110] *See infra* Part IV.
[111] *See infra* Part V.