

Boston College International and Comparative Law Review

Volume 32

Issue 2 *The Pen, the Sword, and the Waterboard:
Ethical Lawyering in the "Global War on Terroism"*


Article 16

5-1-2009

Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense

Matthew Hoisington

Follow this and additional works at: <http://lawdigitalcommons.bc.edu/iclr>

 Part of the [International Law Commons](#), and the [Military, War and Peace Commons](#)

Recommended Citation

Matthew Hoisington, *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, 32 B.C. Int'l & Comp. L. Rev. 439 (2009), <http://lawdigitalcommons.bc.edu/iclr/vol32/iss2/16>

This Comments is brought to you for free and open access by the Law Journals at Digital Commons @ Boston College Law School. It has been accepted for inclusion in Boston College International and Comparative Law Review by an authorized administrator of Digital Commons @ Boston College Law School. For more information, please contact nick.szydowski@bc.edu.

CYBERWARFARE AND THE USE OF FORCE GIVING RISE TO THE RIGHT OF SELF-DEFENSE

MATTHEW HOISINGTON*

Abstract: Cyberwarfare represents a novel weapon that has the potential to alter the way state and non-state actors conduct modern war. The unique nature of the threat and the ability for cyberwar practitioners to inflict injury, death, and physical destruction via cyberspace strains traditional definitions of the use of force. In order to clearly delineate the rights of the parties involved, including the right to self-defense, the international community must come to some consensus on the meaning of cyberwarfare within the existing *jus ad bellum* paradigm. After examining the shortcomings inherent in classifying cyberattacks according to classical notions of kinetic warfare, this Comment argues that international law should afford protection for states who initiate a good-faith response to a cyberattack, especially when the attack targets critical national infrastructure.

INTRODUCTION

Cyberwarfare¹ is a new type of weapon that has the potential to alter modern warfare significantly.² Computer technology has advanced to the point where military forces now have the capability to

* Matthew Hoisington is a Note Editor for the *Boston College International & Comparative Law Review*. He would like to thank Max Matthews, Kyle Robertson, Christian Westra, Nicole Karlebach, Alex Watson, and Matthew Ivey for their attentive editorial assistance in the writing of this comment.

¹ Primarily, I use the terms “cyberwarfare” or “cyberattack” in place of terms such as information warfare, or computer network attack. The terms are often used interchangeably in the literature and for the purposes of this comment can be seen as falling under the same umbrella definition provided in the introduction. In his 2001 report for Congress, Stephen Hildreth defined cyberwarfare broadly as including defending information and computer networks, deterring information attacks, as well as denying an adversary’s ability to do the same. He also included offensive information operations mounted against an adversary, or even dominating information on the battlefield. See STEPHEN HILDRETH, CRS REPORT FOR CONGRESS, CYBERWARFARE 16–17 (2001) available at <http://www.fas.org/irp/crs/RL30735.pdf>.

² See Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U.J. INT’L L. & POL. 57, 57 (2001).

inflict injury, death, and destruction via cyberspace.³ Cyberwarfare can range from relatively innocuous web vandalism to severe attacks on critical national infrastructure.⁴ While the temporary deactivation of government web pages may represent little more than a nuisance, the threat of misinformation spread to military commanders in the field, or a concerted attack on a state's electric, water, communications, transportation, or fuel networks represents a serious risk to both soldiers and civilians.⁵ The infiltration of state information networks and the procurement of classified data—commonly called computer espionage—also fall within the spectrum of cyberwarfare, and are made easier by the increased dependence of state agencies on electronic communications.⁶

Despite the potential lethality of cyberwarfare, the practice currently exists in a legal netherworld.⁷ The highly destructive scenarios, as well as the potential use of cyberwar techniques in asymmetrical warfare, underscore the need for an unambiguous standard of conduct for cyberwarfare that will be universally recognized and respected.⁸ Whether cyberwarfare constitutes a use of force giving rise to the right of self-defense therefore represents an important question in international law.⁹

Modern law on the use of force is based on article 2(4) of the United Nations (U.N.) Charter (Charter); however, the precise definition of what constitutes the use of force is unclear.¹⁰ Neither the Char-

³ 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, 180 (2006).

⁴ See Center for the Study of Technology and Society, *Special Focus: Cyberwarfare*, <http://web.archive.org/web/20061205020720/tecsoc.org/natsec/focuscyberwar.htm> (2001). The authors split cyberwarfare into five general varieties. Ranging from the mildest to the most severe these five are: 1) web vandalism, 2) disinformation campaigns, 3) gathering secret data, 4) disruption in the field, and 5) attacks on critical national infrastructure. See *id.* Other commentators have defined cyberwarfare more generally as any operation that disrupts, denies, degrades, or destroys information resident in computers or computer networks. See WALTER GARY SHARP, *CYBERSPACE AND THE USE OF FORCE* 132 (1999).

⁵ See *Special Focus*, *supra* note 4.

⁶ See *id.*

⁷ See *The Mouse that Roared*, THE ECONOMIST ONLINE, Sept. 5, 2007, http://www.economist.com/daily/news/displaystory.cfm?story_id=9752625&fsrc=nwl; see also HILDRETH, *supra* note 1, at 9 (discussing the applicable legal framework regarding cyberwarfare).

⁸ See Brown, *supra* note 3, at 180–81.

⁹ See generally Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self Defense*, 38 STAN. J. INT'L L. 207 (2002) (emphasizing the importance of classifying computer network attacks on critical national infrastructure as a use of force giving rise to the right of self-defense).

¹⁰ See Barkham, *supra* note 2, at 69–70.

ter nor any international body has defined the term clearly.¹¹ Attempts to define cyberwarfare within the meaning of article 2(4) have strained traditional interpretations further.¹² Analysis of the acceptability under the *jus ad bellum*, the body of international law governing the use of force as an instrument of national policy, of cyberwarfare centers on the Charter's prohibition of the use of force in article 2(4), its Chapter VII security scheme, the inherent right to self-defense codified in article 51, and customary international law as established by the behavior of states.¹³

While a considerable body of international law applies to the use of force by states, its application to cyberspace is not always obvious and many questions remain surrounding precisely how international law relates to cyberwarfare.¹⁴ After a brief look at the history of cyberwarfare, this Comment initially seeks to answer a threshold question: what constitutes a use of force in cyberspace? Discussion addresses the related questions of what qualifies as an armed attack in cyberspace, and whether certain acts of cyberwarfare could constitute a per se use of force.¹⁵ Once the key prescriptions on the use of force are identified, the discussion moves to the right to use force in self-defense, and the circumstances when a state may legally invoke the right. Conclusions in the analysis include the assertion that the prevalence of cyberwarfare will require either an expansion of the application of the article 2(4) definition of the use of force or the development of new means of addressing the threat.

¹¹ See *id.* at 70.

¹² See *id.* at 57; see also Raymond C. Parks & David P. Duggan, Principles of Cyberwarfare, Proceedings of the 2001 IEEE Workshop on Information Assurance and Security (June 5–6, 2001) (examining the differences between cyberwarfare and traditional kinetic warfare).

¹³ See generally Michael N. Schmitt, *Computer Network Attacks and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. TRANSNAT'L L. 885 (1999) (advocating the benefits of fitting cyberattacks within the existing use of force framework).

¹⁴ See SHARP, *supra* note 4, at 7.

¹⁵ See OFFICE OF GEN. COUNSEL, DEP'T OF DEF., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 15 (1999) available at <http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf> [hereinafter DoD OGC]. Read together, the applicable provisions of the Charter and related General Assembly resolutions provide a myriad of terms and concepts concerning prohibited uses of force among nations, including the threat or use of force, acts of aggression, wars of aggression, the use of armed force, invasion, attack, bombardment and blockade. These acts may be directed at the victim nation's territorial integrity or political independence, or against its military forces or marine or air fleets. They all have in common the presence of troops and the use of traditional military weapons. *Id.* The question before this Note is how they are likely to apply to cyberwarfare.

I. BACKGROUND

Cyberattacks present an attractive option to foes of the United States as a form of guerilla or asymmetrical warfare.¹⁶ The specter of an unanticipated and massive attack on critical infrastructures that disables core functions such as telecommunications, electrical power systems, gas and oil, banking and finance, transportation, water supply systems, government services, and emergency services has been raised in a number of reports on national security and by the U.S. National Infrastructure Protection Center (NIPC), as well as other sources within the government.¹⁷

In 1997, Operation *Eligible Receiver* was the first information warfare exercise in the United States to address the issue of cyberwarfare.¹⁸ In the ninety-day exercise, thirty-five people participated on behalf of the rogue state using off-the-shelf technology and software.¹⁹ The scenario assumed a rogue state rejecting direct military confrontation with the United States, seeking instead to attack vulnerable information systems.²⁰ Some of the goals of the rogue state were to conceal the identity of the hackers and to delay or deny any ability by the United States to respond militarily.²¹ A number of simulated attacks were made against power and communications networks in nine major metropolitan areas.²² According to unclassified reports, the government and commercial sites proved susceptible to attack and take-down.²³

In a 2001 Congressional Research Service (CRS) report to Congress, Stephen Hildreth, a national defense specialist from the Foreign Affairs, Defense, and Trade Division urged Congress to critically examine the policies, organization, and legal framework guiding executive branch decision-making on issues of cyberwarfare.²⁴ Hildreth's report examined broad cyberwarfare issues and their underlying questions.²⁵

¹⁶ DEP'T OF DEF., ANN. REP. TO CONG., MILITARY POWER OF THE PEOPLE'S REPUBLIC OF CHINA 13–14 (2007) available at <http://www.defenselink.mil/pubs/pdfs/070523-China-Military-Power-final.pdf> [hereinafter DOD REPORT ON CHINA].

¹⁷ See MICHAEL A. VATIS, INSTITUTE FOR SECURITY TECHNOLOGY STUDIES AT DARTMOUTH COLLEGE, CYBER ATTACKS DURING THE WAR ON TERRORISM: A PREDICTIVE ANALYSIS 17 (2001), http://www.ists.dartmouth.edu/projects/archives/cyber_a1.pdf.

¹⁸ See HILDRETH, *supra* note 1, at 4.

¹⁹ See *id.*; Vatis, *supra* note 17.

²⁰ See HILDRETH, *supra* note 1, at 4.

²¹ See *id.*

²² See *id.*

²³ See *id.*; Vatis, *supra* note 17.

²⁴ See generally HILDRETH (urging Congress to consider the threat seriously and articulating some possible approaches).

²⁵ See *id.* at 1–2.

The report highlighted the pervasiveness and seriousness of the threat, and indicated that the risk of cyberwarfare represented an emerging area of national interest.²⁶

The real-life impact of cyberattacks became obvious in 2007 when Russian hackers unleashed an international cyber-assault on Estonia temporarily shutting down Estonian government computers, after the Baltic country caused offense by re-burying a Russian soldier from the Second World War.²⁷ Some analysts characterized the attack as the first direct Russian assault on a North Atlantic Treaty Organization (NATO) member.²⁸ Again, in 2008, the Russian military sought to employ the weapon of cyberwarfare as a complement to its kinetic invasion of the Abkhazia and South Ossetia regions of neighboring Georgia, this time disabling numerous government websites, including the site for the Georgian Ministry of Foreign Affairs.²⁹

Russia is not alone in utilizing cyberwar techniques as recent reports also indicate that hackers connected to the Chinese army successfully broke into Pentagon computers.³⁰ Pentagon officials speculated that the online intruders were probably engaged in espionage, downloading information.³¹ Some claim that the attacks can be directly attributed to the People's Liberation Army (PLA).³² Germany's government has protested to China's rulers, saying it too was once hacked by the PLA.³³ Given U.S. vulnerabilities, it may only be a matter of time before the country is faced with either a terrorist-sponsored cyberspace equivalent of the September 11th attacks or with a preparatory cyber onslaught in a situation similar to that proposed by Unrestricted Warfare, the Chinese Military manual.³⁴ A Pentagon report in 2007 on

²⁶ See *id.* at 15.

²⁷ See *The Mouse That Roared*, *supra* note 7. The assault was characterized as a "denial of service" attack, whereby huge numbers of simulated visitors overwhelm the website. See *id.*

²⁸ See *id.*

²⁹ See John Markoff, *Georgia Takes a Beating in the Cyberwar with Russia*, N.Y. TIMES ONLINE, Aug. 11, 2008, <http://bits.blogs.nytimes.com/2008/08/11/georgia-takes-a-beating-in-the-cyberwar-with-russia/?scp=1&sq=cyberwarfare&st=cse>.

³⁰ See Stephen Fidler et al., *US Concedes Danger of Cyber-attack*, FINANCIAL TIMES ONLINE, Sept. 7, 2007, at 7, <http://search.ft.com/ftArticle?queryText=People%27s+Liberation+Army%2C+computer&aje=false&id=070905010503&ct=0>.

³¹ See *id.*; *The Mouse That Roared*, *supra* note 7.

³² See Lewis Page, *Pentagon: Chinese Military Hacked Us*, THE REGISTER ONLINE, Sept. 4, 2007, http://www.theregister.co.uk/2007/09/04/china_hack_pentagon_leak/; *The Mouse That Roared*, *supra* note 7.

³³ See *The Mouse That Roared*, *supra* note 7.

³⁴ See Jensen, *supra* note 9, at 213; see also Daniel M. Creekman, *A Helpless America? An Examination of the Legal Options Available to the United States in Response to Various Cyber-attacks from China*, 17 AM. U. INT'L L. REV. 641, 670-71 (2002) (discussing the Chinese emphasis

China's military force indicates that the country is developing tactics to achieve electromagnetic dominance early in a conflict.³⁵ It adds that China, while not yet having a formal doctrine of electronic warfare, has begun to consider offensive cyberattacks within its operational exercises,³⁶ and is moving aggressively toward incorporating cyberwarfare into its military lexicon, organization, training, and doctrine.³⁷

To the extent that national leaders are unlikely to allow such a catastrophic intrusion upon their sovereignty without a response involving more than diplomatic protests, determining what legal responses are available represents a key inquiry into the nature and international legal implications of cyberwarfare.³⁸

II. DISCUSSION

A. *Cyberwarfare, Treaty Law, and International Norms*

In 1999, the U.S. Department of Defense produced a document that examined the range of treaties and international law that might pertain to the conduct of cyberwarfare, supplementing the various U.S. laws guiding the conduct of warfare in general and U.S. government conduct in cyberspace.³⁹ The assessment concluded first that the international community is unlikely to promptly produce a coherent body of law on the subject.⁴⁰ Second, no clear legal remedies exist to address the type of cyberwarfare operations being considered by the United States.⁴¹ Third, the document recommended analyzing the various elements and circumstances of any particular planned operation or activity to determine the applicability of existing international legal principles.⁴²

on their ability to wage information warfare and the country's open contemplation of the development of a fourth branch of the armed services dedicated to information warfare).

³⁵ See *The Mouse That Roared*, *supra* note 7. See generally DOD REPORT ON CHINA, *supra* note 16 (outlining the different capabilities of the Chinese military and the general Chinese approach to foreign policy).

³⁶ See DOD REPORT ON CHINA, *supra* note 16, at 16; *The Mouse That Roared*, *supra* note 7.

³⁷ See HILDRETH, *supra* note 1, at 12; Creekman, *supra* note 34, at 652–53 & 670–71.

³⁸ See Jensen, *supra* note 9, at 213–14.

³⁹ See HILDRETH, *supra* note 1, at 9. See generally DoD OGC, *supra* note 15 (examining the legal landscape regarding cyberwarfare).

⁴⁰ See DoD OGC, *supra* note 15, at 50; HILDRETH, *supra* note 1, at 9.

⁴¹ See HILDRETH, *supra* note 1, at 9.

⁴² See DoD OGC, *supra* note 15, at 50; HILDRETH, *supra* note 1, at 9.

A number of existing international treaties suggest norms which could ultimately be used to regulate cyberwarfare.⁴³ The International Telecommunications Convention (ITC), for instance, prohibits harmful interference with telecommunications.⁴⁴ While the effectiveness of the treaty is limited by its state security exception, the creation of a norm analogizing network space to airspace could prove vital to the development of international law in cyberspace.⁴⁵ Of course, a violation of the ITC does not constitute a *per se* use of force within the meaning of article 2(4) of the Charter and therefore does not necessarily generate the same opposition within the international community as other clear-cut acts of aggression.⁴⁶

Another potentially relevant international legal document is the Agreement on the Prevention of Dangerous Military Activities, signed by the United States and the Soviet Union in 1989. This treaty prohibits harmful interference with enemy command and control systems, therefore suggesting a possible emergent norm that could designate cyberwarfare attacks as a use of force.⁴⁷

In the 1990s as the concept of cyberwarfare first began to receive widespread attention from the media, there were some efforts within the international community to negotiate an agreement.⁴⁸ Russia tabled a resolution in the U.N.'s First Committee in October 1998 in an apparent effort to get the U.N. to focus on the subject.⁴⁹ The resolution included a call for states to support their views regarding the advisability of elaborating international legal regimes to ban the development, production, and use of particularly dangerous information weapons.⁵⁰ The initiative, however, found little support among the international community, and was never submitted to the General Assembly for a plenary vote.⁵¹

As a result of the failure of the international community to produce a directly applicable international agreement key legal issues regarding cyberwarfare remain unresolved.⁵² These include, for example, the need for standards informing the expeditious pursuit of those violating

⁴³ See Barkham, *supra* note 2, at 95.

⁴⁴ See *id.*

⁴⁵ See *id.* at 95–96.

⁴⁶ See *id.* at 96.

⁴⁷ See *id.*

⁴⁸ See DoD OGC, *supra* note 15, at 49.

⁴⁹ See *id.*

⁵⁰ See *id.*

⁵¹ See *id.*

⁵² See Barkham, *supra* note 2, at 96–97.

the law, law enforcement needs in the conduct of electronic surveillance of those launching cyberattacks, and the establishment of clear and appropriate rules of engagement for cyber defense activities.⁵³

B. *Cyberwarfare and International Law on the Use of Force*

Any number of purposes might motivate a state to conduct cyberwarfare and regardless of the aim the normative evaluation by the international community will center on whether the cyberattacks, both offensive and retaliatory, constituted a wrongful use of force, or threat thereof, in violation of international law.⁵⁴ In order to define cyberwarfare effectively, the international community must come to some consensus on the meaning of such activities within the penumbra of the Charter, specifically article 2(4) regulating the use of force, and article 51, which outlines the right of self-defense.⁵⁵

Article 2(4) of the Charter expresses the key prescription in international law regarding the use of force.⁵⁶ The provision states 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 in any other manner inconsistent with the Purposes of the United Nations.”⁵⁷ Given this analytical framework, the dispositive question is whether an act constitutes a use of force.⁵⁸ The Charter clearly outlaws the aggressive use of force, while recognizing a state’s inherent right of individual and collective self-defense in article 51.⁵⁹ Accordingly, if a state activity constitutes a use of force within the meaning of article 2(4), it is unlawful unless it is an exercise of that state’s inherent right of self-defense.⁶⁰

⁵³ See *id.*

⁵⁴ See Schmitt, *supra* note 13, at 900.

⁵⁵ See Creekman, *supra* note 34, at 679. See generally SHARP, *supra* note 4 (articulating an approach that defines acts of cyberwarfare within the existing *ius ad bellum*).

⁵⁶ See *id.*

⁵⁷ U.N. Charter, art. 2, para. 4.

⁵⁸ See Schmitt, *supra* note 13, at 904.

⁵⁹ See SHARP, *supra* note 4, at 33.

⁶⁰ See *id.* at 33–34. In addition to the inherent right of self-defense codified under article 51, under article 39 the Security Council has the obligation to maintain or restore international peace. Therefore, articles 2(4), 39, and 51 must be read together to determine the scope and content of the Charter’s prohibition on the aggressive use of force, the responsibility of the Security Council to enforce this prohibition, and the right of all states to use force in self-defense. For the purposes of this paper, discussion of article 39 has been omitted; however, Sharp articulates the relevance of article 39 eloquently in his book. See *id.* at 27–54.

While the precise definition of what constitutes the use of force is unclear, some of the parameters are well-defined.⁶¹ For instance, conventional weapons attacks are included within the article 2(4) definition.⁶² Furthermore, cyberattacks intended to directly cause physical damage to tangible property or injury or death to human beings are reasonably characterized as a use of armed force and, therefore, encompassed in the prohibition.⁶³ Conversely, despite attempts by developing states to include economic coercion within article 2(4) during the drafting of the Charter, such practices have been expressly excluded.⁶⁴ Thus, analysis based on either the text of article 2(4) or the history underlying its adoption requires an interpretation excluding economic, and for that matter political, coercion from the article's prescriptive sphere.⁶⁵

The potential application of article 2(4) to cyberwarfare creates serious interpretive difficulties for the existing distinction between force and coercion.⁶⁶ Including all cyberwarfare actions within the definition of use of force would require a major expansion of article 2(4).⁶⁷ Such an expanded definition of the use of force would make it very difficult to continue to exclude acts of coercion from article 2(4) because international law would have to distinguish cyberattacks that do not cause physical damage, such as electronic incursions and blockades, from acts of economic and political coercion, such as economic sanctions, which traditionally and specifically have been excluded from article 2(4), but which may often have the same effect.⁶⁸ The dilemma lies in classifying cyberattacks that do not cause physical damage, or do so indirectly, *vis-à-vis* the prohibition on the use of force.⁶⁹

⁶¹ See Barkham, *supra* note 2, at 70.

⁶² See *id.*; Schmitt, *supra* note 13, at 904.

⁶³ See Schmitt, *supra* note 13, at 913.

⁶⁴ See Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places?*, 51 NAVAL L. REV. 132, 134–35 (2005); Barkham, *supra* note 2, at 70–71. Defining cyberattacks on economic centers of gravity as use of force under the current international regimes has grave potential for unintended and undesirable legal consequences. Incorporating cyberattacks on critical economic infrastructures into the definition of use of force cannot be done with sufficient precision to exclude other state economic policies which have long been defended as necessary tools of foreign policy, and deliberately excluded from the international definition of the use of force, particularly by market based democracies. See Antolin-Jenkins, *supra*.

⁶⁵ See Schmitt, *supra* note 13, at 905.

⁶⁶ See Barkham, *supra* note 2, at 84.

⁶⁷ See *id.*

⁶⁸ See *id.* at 84–85.

⁶⁹ See Schmitt, *supra* note 13, at 913.

In an attempt to solve this classification impasse, Michael Schmitt delimits economic and political coercion from the use of armed force by reference to six criteria: 1) severity, 2) immediacy, 3) directness, 4) invasiveness, 5) measurability, and 6) presumptive legitimacy.⁷⁰ Through this scheme, the consequences of the act of cyberwarfare are measured against commonalities to ascertain whether they more closely approximate consequences of the sort characterizing armed force or whether they are better placed outside the use of force boundary.⁷¹ According to Schmitt, this technique allows the force “box” to expand to fill gaps resulting from the emergence of coercive possibilities enabled by technological advances without altering the balance of the current framework.⁷² Instead, the expansion of the use of force definition is cast in terms of the underlying factors driving the existing classifications.⁷³

Applying Schmitt’s technique, in determining whether an a cyber-attack falls within the more flexible consequence-based understanding of force, the nature of the act’s reasonably foreseeable consequences are assessed to determine whether they resemble those of an armed attack.⁷⁴ If the consequences resemble those of an armed attack, extension of the use of force prohibition to the act is justified.⁷⁵ If not, wrongfulness under international law would have to be determined by resort to prescriptions other than those prohibiting force.⁷⁶

An even less onerous, purely result-oriented test represents another potential framework for determining whether specific acts of cyberwarfare constitute a use of force.⁷⁷ Under the strict results-oriented approach no difference exists between an attacker firing a missile at a target or using a computer to remotely cause physical damage.⁷⁸ If a cyberattack achieves the same result that could have been achieved with bombs or bullets, it will be treated the same under international law governing the use of force.⁷⁹ The problem with the result-oriented ap-

⁷⁰ See *id.* at 915.

⁷¹ See *id.*; Antolin-Jenkins, *supra* note 64, at 170.

⁷² See Schmitt, *supra* note 13, at 915.

⁷³ See *id.*

⁷⁴ See *id.* at 915–16.

⁷⁵ See *id.* at 916.

⁷⁶ See *id.*; see also Antolin-Jenkins, *supra* note 64, at 170 (recognizing the gray areas that result from the consequence based approach, as opposed to the bright line rules provided by an instrument-based analysis).

⁷⁷ See Barkham, *supra* note 2, at 86.

⁷⁸ See Brown, *supra* note 3, at 187.

⁷⁹ See *id.*

proach to cyberattacks is that it blurs the distinction excluding economic coercion from the traditional use of force classification characterized by armed attacks, since economic coercion could also serve as the proximate cause of disruptive or destructive effects.⁸⁰

C. *Cyberwarfare and the Self-Defense Exception*

Under the Charter, there are two exceptions to the prohibition on the use of force: Security Council action pursuant to article 42, and individual or collective self-defense under article 51.⁸¹ Legal scholars disagree on the current state of customary international law as it relates to the use of force in self-defense and the proper interpretation of article 51.⁸² Article 51 of the Charter states:

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 the measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence 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.⁸³

The scope of article 51 represents the subject of considerable controversy among international legal scholars.⁸⁴ Some scholars interpret article 51 strictly, arguing that a state may not act in self-defense until that state has suffered an armed attack.⁸⁵ According to this reading, a state

⁸⁰ See Barkham, *supra* note 2, at 86.

⁸¹ See Sean M. Condon, *Getting it Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J. L. TECH. 403, 413 (2007). Article 42 of the U.N. Charter states, "Should the Council consider that measures provided for in article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. See U.N. Charter arts. 41–42. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of the Members of the United Nations." *Id.*

⁸² See Condon, *supra* note 81.

⁸³ U.N. Charter art. 51.

⁸⁴ See Barkham, *supra* note 2, at 74; Condon, *supra* note 81, at 412–13.

⁸⁵ See Condon, *supra* note 81, at 412; see also Barkham, *supra* note 2, at 74–75 (describing the Security Council view of article 51 as restrictive, declining to approve of actions taken that were not in specific response to an armed attack).

could not act in anticipation of an armed attack.⁸⁶ Nevertheless, a great many states take the counter-restrictionist view and support the proposition that in certain circumstances it may be lawful to use force in advance of an actual armed attack.⁸⁷ Legal scholars supporting the latter stance argue that article 51 incorporates customary international law as articulated by the *Caroline* standard, allowing anticipatory self-defense.⁸⁸ As defined by then Secretary of State, Daniel Webster in the *Caroline* case, this point in time occurs when the “necessity of that self-defence is instant, overwhelming and leaving no choice of means, and no moment for deliberation.”⁸⁹

Under the *jus ad bellum* paradigm, a state response to an armed attack must meet three conditions to qualify as self-defense: necessity, proportionality, and immediacy.⁹⁰ To fulfill the principle of necessity the state must attribute the attack to a specific source, characterize the intent behind the attack, and conclude that the state must use force in response.⁹¹ The principle of proportionality requires that the force used in the response be proportional to the original attack.⁹² The requirement of immediacy prohibits a response from occurring after too much time has passed.⁹³ With regard to immediacy as a general criterion, however, no requirement exists for defensive action to be exercised (or risk forfeiture), immediately following an armed attack.⁹⁴

⁸⁶ See Condrón, *supra* note 81, at 412.

⁸⁷ See ANTHONY C. AREND & ROBERT J. BECK, INTERNATIONAL LAW AND THE USE OF FORCE: BEYOND THE UN CHARTER PARADIGM 79 (1993); see also DoD OGC, *supra* note 15, at 15–16 (examining the well-established view that article 51 did not create the right of self-defense, but that it only recognized a preexisting inherent right that is in some respects broader than the language of article 51); William H. Taft IV, *International Law and the Use of Force*, 36 GEO. J. INT’L L. 659 (2005) (articulating the U.S. approach to preemption and asserting that states have a well established right to use force before an actual attack has taken place so long as the attack is imminent).

⁸⁸ See Condrón, *supra* note 81, at 412–13; see also DoD OGC, *supra* note 15, at 16 (discussing the *Caroline* doctrine and its venerable roots in United States’ foreign policy).

⁸⁹ Letter from U.S. Secretary of State, Daniel Webster, to Lord Ashburton (Aug. 6, 1842) available at <http://www.yale.edu/lawweb/avalon/diplomacy/britain/br-1842d.htm>.

⁹⁰ See Condrón, *supra* note 81.

⁹¹ See *id.*

⁹² See *id.*; see also SHARP, *supra* note 4, at 39 (defining proportionality within the law of armed conflict as that level of force required to destroy a military objective but which does not cause unnecessary collateral destruction of civilian property or unnecessary human suffering of civilians).

⁹³ See Condrón, *supra* note 81, at 414.

⁹⁴ See T.D. Gill, *The Temporal Dimension of Self-Defence: Anticipation, Pre-emption, Prevention and Immediacy*, 11 J. CONFLICT & SECURITY L. 361, 369 (2006).

Attribution and characterization are especially important in context of cyberwarfare.⁹⁵ Generally, the international law of self-defense does not justify acts of active defense across international borders unless the provocation can be attributed to an agent of the nation concerned.⁹⁶ Given the opportunities cyberspace creates for the remote commission of attacks and attacker anonymity, perpetrators of cyberattacks are likely to go unidentified.⁹⁷ Attribution helps to ensure that a state does not target an innocent person or place.⁹⁸ Furthermore, a state must attribute an attack because the laws governing a permissible response vary depending on whether the attacker is a state actor or a non-state actor.⁹⁹ The article 2(4) prohibition on the use of force generally applies only to states and not to individuals.¹⁰⁰ States, therefore, are prevented under international law from threatening or using force against each other, while similar acts by individuals fall under the province of domestic criminal laws.¹⁰¹

While it is difficult to discover the identity of the attacker, identifying his or her intent in time to take preventive action represents an equally problematic and potentially more important task.¹⁰² In order to respond with force, a victim state must first identify the attacker's intentions as hostile.¹⁰³ Unlike conventional kinetic warfare, the instantaneous nature of a cyberattack deprives the victim state of the opportunity to preemptively contemplate a response.¹⁰⁴ As a solution, Walter Gary Sharp has proposed that all states should adopt a rule of engagement that allows them to use force in anticipatory self-defense against any identified state that demonstrates hostile intent by penetrating a computer system which is critical to their respective vital national interests.¹⁰⁵

⁹⁵ See Condrón, *supra* note 81, at 414. See generally Susan Brenner, "At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare, 97 J. CRIM. LAW & CRIMINOLOGY 379 (2007) (discussing the difficulty of attributing cyberattacks due to the unique quickness of the attack).

⁹⁶ See DoD OGC, *supra* note 15, at 22.

⁹⁷ See Brenner, *supra* note 95, at 380.

⁹⁸ See Condrón, *supra* note 81, at 414.

⁹⁹ See *id.*; Jensen, *supra* note 9, at 232–33.

¹⁰⁰ See Jensen, *supra* note 9, at 232.

¹⁰¹ See *id.* at 232–33.

¹⁰² See *id.* at 235. Jensen discusses identifying the intent of the attacker under the sub-heading "Characterization of the Attack." *Id.*

¹⁰³ See *id.*

¹⁰⁴ See *id.*

¹⁰⁵ See SHARP, *supra* note 4, at 130.

III. ANALYSIS

Existing attempts at defining cyberwarfare within the current *jus ad bellum* paradigm fail to offer adequate safeguards from cyberattacks.¹⁰⁶ The technology inherent in cyberwarfare makes it nearly impossible to attribute the attack to a specific source or to characterize the intent behind it.¹⁰⁷ Furthermore, acts of cyberwarfare occur almost simultaneously.¹⁰⁸ A legal system that requires a determination of the attacker's identity and intent does not account for these features of the digital age.¹⁰⁹ The current international paradigm therefore limits the options available to states, making it difficult to effectively respond without risking a violation of international law.¹¹⁰ Restraining a state's ability to respond will encourage rogue nations, terrorist organizations, and individuals to commit increasingly severe cyberattacks.¹¹¹

Serious flaws exist in Michael Schmitt's consequence-based framework for analyzing cyberwarfare under article 2(4).¹¹² By using presumptive legitimacy as a factor, Schmitt's approach requires determining the legitimacy of an attack under international law by asking whether the attack is legitimate.¹¹³ In effect, the approach is backwards.¹¹⁴ Furthermore, unlike other types of warfare, instances of cyberwarfare cannot be assessed readily at the time of the attack to determine their magnitude and the permitted responses.¹¹⁵ This problem will arise with any framework that requires an *ex post* analysis, including the aforementioned results-oriented approach.¹¹⁶

¹⁰⁶ See Condron, *supra* note 81, at 414. See generally Antolin-Jenkins, *supra* note 64 (proposing an approach using the non-intervention doctrine); Barkham, *supra* note 2 (advocating an expansion of article 2(4) interpretations to address the threat of information warfare); Jensen, *supra* note 9 (emphasizing the importance of providing some recourse for states subject to cyberattacks on critical national infrastructure).

¹⁰⁷ See Condron, *supra* note 81, at 415; Jensen, *supra* note 9, at 232.

¹⁰⁸ See Condron, *supra* note 81, at 415; Jensen, *supra* note 9, at 239–40.

¹⁰⁹ See Condron, *supra* note 81, at 415; Creekman, *supra* note 34, at 680.

¹¹⁰ See DoD OGC, *supra* note 15, at 17; Condron, *supra* note 81, at 415; Creekman, *supra* note 34, at 668–69.

¹¹¹ See Jensen, *supra* note 9, at 228.

¹¹² See Antolin-Jenkins, *supra* note 64, at 172; Barkham, *supra* note 2, at 85–86.

¹¹³ See Barkham, *supra* note 2, at 86. Barkham notes that the primary determination in assessing the legitimacy of an attack under international law rests in distinguishing between acts of coercion and uses of force. By using legitimacy as a factor, Schmitt ties himself into a knot. If the question is whether cyberwarfare is a use of force or coercion, and coercion is legitimate and force is not, the we cannot ask whether the action is legitimate to determine whether the action is force or coercion. See *id.*

¹¹⁴ See *id.*

¹¹⁵ See Barkham, *supra* note 2, at 86; Jensen, *supra* note 9, at 239–40.

¹¹⁶ See Barkham, *supra* note 2, at 86.

To address the unique nature of cyberwarfare, international law should afford protection for states who initiate a good-faith response to an attack, thus acting in cyber self-defense, without first attributing and characterizing the attack.¹¹⁷ State survival may depend on an immediate, robust, and aggressive response; therefore international law should not impose an inflexible requirement on states to fully satisfy the traditional necessity requirements when acting in self-defense of vital state interests.¹¹⁸ The law should evolve to recognize a state's inherent right to self-defense, including anticipatory self-defense, in response to a cyberattack, especially when the attack targets critical national infrastructure.¹¹⁹

Allowing a state to exercise active defense measures in response to an attack on critical national infrastructure, without incurring liability, represents a preferable governing principle to the treatment of cyberwarfare under the existing *jus ad bellum* paradigm.¹²⁰ In order to delineate this exception to the usual rule governing the use of force, the international community should promulgate a list of critical national infrastructure that a state may protect with active defense measures.¹²¹ If the critical infrastructure identified on the list were subjected to a cyberattack, a state could respond in presumptively good-faith self-defense without first attributing or characterizing the attack to the level of specificity required under the traditional formulation.¹²² Such an exception would not fundamentally alter the *jus ad bellum* framework,

¹¹⁷ See Condrón, *supra* note 81, at 415.

¹¹⁸ See *id.*; Jensen, *supra* note 9, at 239–40.

¹¹⁹ See Creekman, *supra* note 34, at 677–78; Jensen, *supra* note 9, at 229. Creekman mentions in his article that while the clarification of article 2(4) may deter states from conducting cyberwarfare, the certainty of the response serves as the ultimate deterrent. Somewhat similar to the mutually assured destruction theory of preventing nuclear war, a clear policy that cyberattacks are met with the severest responses, both conventionally and electronically, serves to outweigh potential benefits that arise from instigating the initial cyberattack. See Creekman, *supra* note 34, at 677–78.

¹²⁰ See Condrón, *supra* note 81, at 416.

¹²¹ See *id.*; Creekman, *supra* note 34, at 654–55. The United States has enumerated, to a certain extent, those targets which may be included on a list of critical national infrastructure. Vital targets are those computer systems related to five critical infrastructures identified by the President's Commission on Critical Infrastructure Protection, charged with assessing the nation's vulnerability to computer attacks. The Commission determined that the United States has five critical infrastructures—Information and Communications, Physical Distribution, Energy, Banking and Finance, and Vital Human Services—whose incapacity or destruction would cripple the nation's defensive or economic security. Such a list could serve as a model for any international cooperative effort addressing self-defense to cyberattacks on critical national infrastructure. See Creekman, *supra* note 34, at 654–55.

¹²² See Condrón, *supra* note 81, at 416.

but would instead allow the state to exercise its inherent right of self-defense in response to a novel threat.¹²³

CONCLUSION

The U.N. Charter was written before the internet existed and, therefore, cyberwarfare presents a unique challenge to traditional definitions of what constitutes a use of force. Despite this difficulty, the serious and pervasiveness of the threat demand that the international community come to a consensus on both the meaning of cyberwarfare within the *jus ad bellum* paradigm, and the options available to states subjected to cyberattack. Serious threats to international peace will result unless states have the ability to respond in self-defense to cyberattacks without being restrained by outdated interpretations of international law governing the use of force.

¹²³ See *id.* But see Antolin-Jenkins, *supra* note 64, at 173–74 (advocating an approach which places cyberattacks into a framework of non-intervention as opposed to modifying the existing use of force formulation).