Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense

Eric Talbot Jensen
BYU Law, jensene@law.byu.edu

Follow this and additional works at: https://digitalcommons.law.byu.edu/faculty_scholarship

Part of the Computer Law Commons, and the National Security Law Commons

Recommended Citation

This Article is brought to you for free and open access by BYU Law Digital Commons. It has been accepted for inclusion in Faculty Scholarship by an authorized administrator of BYU Law Digital Commons. For more information, please contact hunterlawlibrary@byu.edu.
Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense

ERIC TALBOT JENSEN*

If the attacking side secretly musters large amounts of capital without the enemy nation being aware of this at all and launches a sneak attack against its financial markets, then after causing a financial crisis, buries a computer virus and hacker detachment in the opponent's computer system in advance, while at the same time carrying out a network attack against the enemy so that the civilian electricity network, traffic dispatch network, financial transaction network, telephone communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots and a political crisis. There is finally the forceful bearing down by the army, and military means are utilized in gradual stages until the enemy is forced to sign a dishonorable peace treaty.¹

The strategy in this Chinese army publication, Unrestricted Warfare, is to use common computer hacker tools (Trojan horses, logic bombs, viruses, worms,

---


The author wishes to express his gratitude to Lt. Col. Michael Jordan, USMC, for his invaluable advice and direction on the Article.

The views expressed in this Article are those of the author and do not represent the views of the Department of Defense or the Department of the Army.

denials of service, code breaking, etc.)\(^2\) along with a dedicated hacker detachment to paralyze enemy computer networks and erode civilian infrastructure and life support. After these initial measures have produced the desired effect, the attacking country will use its military to defeat the debilitated victim.

This strategy illustrates the most important questions in the computer network attack (CNA)\(^3\) and computer network defense (CND)\(^4\) debates. Is an attack on a nation's computer network system an illegal use of force within the meaning of the United Nations Charter\(^5\) or customary international law?\(^6\) Does such an attack trigger a nation's right to self-defense? Or must a nation wait for a more traditional military attack?

This Article will examine these issues and propose that international law must evolve to recognize that attacks against a nation's critical national

\(^2\) See generally DOROTHY E. DENNING, INFORMATION WARFARE AND SECURITY (2000) (describing the common computer hacker tools employed in information warfare and possible defense strategies). A detailed description of these techniques is beyond the scope of this Article. However, a brief introduction to some standard hacker tools is valuable as a baseline for the discussion that follows. A Trojan horse is a “program that, when activated, performs some undesirable action not anticipated by the person running it. It could delete files, reformat a disk, or leak sensitive data back to its author.” \textit{Id.} at 259. A logic bomb, or time bomb, is a Trojan horse that is “triggered by some event.” \textit{Id.} at 259.

A virus is a fragment of code that attaches itself to other computer instructions, including software application code... performs some function and then turns control over to its host. ... The resident copy watches for uninfected hosts [and] inserts a copy of itself in the host. The virus may then execute a “payload,” which can do anything from displaying an amusing or political message to wiping out files on the hard drive. \textit{Id.} at 269–70.

A worm is a program that propagates from one computer to another over a computer network by breaking into the computers in much the way that a hacker would break into them. Unlike viruses, they do not get any help from unwitting users. They must find a computer they can penetrate, carry out an attack, and transfer a replica of their code to the target host for execution. In effect, a worm completely automates the steps taken by a computer intruder who hops from one system to the next. \textit{Id.} at 280. Denial of service attacks deny legitimate users access to information sources by destroying data or disrupting operations. \textit{Id.} at 231. Code breaking entails “acquiring access to the plaintext of encrypted data by some means other than the normal decryption process used by the intended recipient(s) of the data. Code breaking is achieved either by obtaining the decryption key through a special key recovery service or by finding the key through cryptanalysis.” \textit{Id.} at 408; see also George K. Walker, Information Warfare and Neutrality, 33 \textit{VAND. J. TRANSNAT'L L.} 1079, 1100–01 (2000) (defining common hacker tools).

\(^3\) THE JOINT CHIEFS OF STAFF, JOINT PUB. NO. 3-13, JOINT DOCTRINE FOR INFORMATION OPERATIONS 1-9 (Oct. 9, 1998), available at http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf (defining computer network attack as “operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA”).

\(^4\) As used in this Article, computer network defense will mean measures, active or passive (discussed \textit{infra}), which prevent or safeguard the computer or network from the actions of computer network attack. Together, CNA and CND constitute CNO, or computer network operations. In the Pentagon’s 1999 Unified Command Plan, CND was assigned to U.S. Space Command. The next year, Space Command was also given responsibility for CNA; and in April of 2001, Joint Task Force CND was changed to become Joint Task Force CNO. Michael C. Sirak, Threat to the Nets, \textit{A.F. MAG.}, Oct. 2001, at 24.

\(^5\) U.N. CHARTER, reprinted in 3 BEVANS 1153.

\(^6\) Source: Custom, 1 Hackworth DIGEST § 3, at 15–17.
infrastructure from any source constitute a use of force. Such attacks, therefore, give the victim state the right to proportional self-defense—including anticipatory self-defense—even if the CNA is not an armed attack under Article 51 of the United Nations Charter. Due to the instantaneous nature of CNAs, the right to respond must accrue immediately, despite the traditional obstacles of attribution (determining the attacker's identity), characterization (determining the attacker's intent), and the inviolability of neutrals.

I. COMPUTER NETWORK RELIANCE AND VULNERABILITY

On December 29, 2000, CNN.com published a Computerworld report detailing an October 2000 computer hack7 at the Microsoft Corporation.8 Based on a report9 by the Center for Strategic and International Studies (CSIS), the article detailed how Microsoft security personnel discovered the hack when they noticed passwords being sent to a Russian email account. The hackers had gained access to Microsoft's internal network by posing as Microsoft employees working offshore rather than at the company's Redmond, Washington headquarters.10 The hackers may have accessed Microsoft's software source code,11 enabling them to either alter program operation or to install a number of hacker tools into the software. Such alterations may later allow these hackers access into computers and networks that run Microsoft software.

Despite Microsoft's denial of serious damage,12 the CSIS report argues “[i]f this could happen to Microsoft, then no company is safe.”13 Recent

---

7 For the purposes of this Article, a “hacker” is someone who conducts a computer hack, or “gain[s] access to or break[s] into electronic systems, particularly computers and telecommunications systems” and “includes ‘crackers,’ who break access codes and computer locks, and ‘phreakers,’ who crack and exploit phone systems.” DENNING, supra note 2, at 44.
9 BORCHGRAVE ET AL., supra note 1, at iv.
10 Verton, supra note 8.
11 Source code is defined as the “[w]ritten instructions for a program in a form readable by humans. Must be translated or compiled into object code in order to be executed by a computer.” MARK A. LEMLEY ET AL., SOFTWARE AND INTERNET LAW 1098 (2000).
12 Microsoft strongly disagreed with CSIS’s report. Verton, supra note 8. A Microsoft spokesman further stated:

[A]fter tracking the intruders and investigating their activities, there is no evidence and no basis to believe that they had any access at all to Windows or Office source code. That is, we have no reason to believe that the intruders were able to see Windows or Office source code, much less modify it. Microsoft’s current and future products remain intact and secure, and customers can use them with confidence.

Id.
13 BORCHGRAVE ET AL., supra note 1, at iv.
evidence affirms this view. According to the report, if someone can hack into the “heart of the ubiquitous Windows program [they] can hack into any PC in the world that uses it and is connected to the Internet.” In addition, the report stresses the potential danger in the specific programs used:

More troubling still is the admission that the hackers used a relatively unsophisticated program [called a Trojan horse] to penetrate the security perimeter of the world’s most powerful software company. With most military and government systems powered by Microsoft software and more generally reliant on [commercial off-the-shelf hardware and software], this recent development can pose grave national security-related concerns.

The report then uses the Microsoft attack to illustrate a more general vulnerability to cyber attack. This same intrusive capability poses a significant threat to governments as well as to the private sector:

Global computer networks make it easier for the new, flexible networks like Osama Bin Laden’s al-Qaida to communicate in heavily encrypted secrecy and organize without building a vulnerable central [headquarters].

The capacity to produce, communicate and use information is affecting every area of national security, from the way we govern ourselves, [1] to the way we fight wars [], to the way transnational criminal organizations increase in size, scope and power, to the way activists and extremists mobilize support across borders. Worms, viruses, Trojan horses, logic bombs, trap doors, denial of service (DOS) attacks, malicious code, all are now weapons in a new geopolitical calculus whereby the sub-state or non-state, or even individual actor, can now aspire to leveling the playing field with the superpower.

The frequency of computer hacker attacks is staggering. In 1999, 22,144 attacks against Department of Defense (DOD) computers were detected, a threefold increase over the previous year. After leveling out between 22,000

14 John Schwartz & Ariana Eunjung Cha, Respite Follows Hacker Attacks; Vandals Pursued by Law and Peers, WASH. POST, Feb. 11, 2000, at E1 (cataloging a number of large U.S. companies that have been the object of recent hacking).

15 BORCHGRAVE ET AL., supra note 1, at iv.

16 Id. at 7.

17 Id. at i–ii.

18 Id. at 9; see also Jim Wolf, Hacking of Pentagon Computers Persists, WASH. POST, Aug. 9, 2000, at 23 (reporting that of those 22,144 attacks, “all but 1,000 of [1999’s] reported attacks were attributed to recreational hackers”). “According to Interpol, 30,000 hacker web sites currently exist on the Internet. In the ten years between 1989 and 1999, there were only 34,000 reported global hacking incidents in aggregate, but between January and October 2000 alone, 50,000 incidents were reported . . . So far this year, the number of attacks is up roughly 10 percent, with over 14,000 electronic attacks detected in the first seven months of the year alone.” BORCHGRAVE ET AL., supra note 1, at 9; see also Elinor Mills Abreu, Israel, US Leading Sources of Cyber Attacks, JERUSALEM POST, Jan. 29, 2002, at 11 (Economics Section), where the author states: “The study found attacks that appeared to originate in the US—nearly 30% of the total—were nearly triple the second-ranked country. But only about 3.5
and 23,000 per year, DOD computer intrusions “are expected to reach 40,000 [in 2001], and they are increasing in complexity and destructiveness.” Even more alarming is that “the Computer Emergency Response Team (CERT) Coordinating Center at Carnegie Mellon has estimated that only 10 percent of attacks are detected, and far fewer are reported.” If this estimate is accurate, over 220,000 attempted intrusions into DOD computers took place in 1999, and over 400,000 would have taken place in 2001. Coupled with the fact that “95 percent of the U.S. military traffic moves over civilian telecommunications and computer systems, our reliance on information systems has become a strategic vulnerability.”

This vulnerability has not gone unnoticed in Washington, D.C. In 1999, Richard Clarke, then the National Coordinator for Security Infrastructure Protection and Counter-terrorism with the National Security Council and currently the special advisor on cyberspace security to President George W. Bush, noted the dangers of computer attacks:

The second type of new threat that ... President [Bill Clinton] has identified as a way of getting at the United States, here at home, and getting at our weaknesses is what has been variously called cyber attack or information warfare, an attack on our infrastructure not from bombs but with computers.

Clarke’s argument is that the United States is very much at risk, not only from amateurs and nonmalicious intruders, but also from sources watching attacks were made per 10,000 US Internet users, compared with 26 attacks per 10,000 Internet users in Israel.” The author also states that this rate for Israel of hacks per ten-thousand Internet users is the highest for any country, followed by Hong Kong, Thailand, South Korea, France, Turkey, Malaysia, Poland, Taiwan, and Denmark. 


20 BORCHGRAVE ET AL., supra note 1, at 9.


22 BORCHGRAVE ET AL., supra note 1, at 10.


24 Id. at 36.

I can tell you that there are tonight nations around the world who are developing or have developed offensive information warfare tools and techniques and have offensive information warfare organizations. I can tell you that those nations are doing reconnaissance today on America’s computer networks looking for our weaknesses, and our vulnerabilities. It is not science fiction.

Id.

25 Id. at 37.

In February of 1998, when Saddam Hussein was defying the UN and the UN Special Commission on Iraq, the President decided to send wings of aircraft to the Persian Gulf. That was on a Friday. On Saturday, we discovered that, at over 20 of our Air Force bases, someone
and waiting for the right time to unleash attacks. The end result would be a frightening one for U.S. civilians:

I suggest to you that one day when the United States is sending forces to stand up against Saddam Hussein, to protect Israel, to protect Taiwan, or to stand somewhere in the world in favor of U.S. interests, that we may experience on that day an electronic Pearl Harbor. We may find that one or two or three of our cities does [sic] not have power, does not have telecommunications, or the railroad system has derailed all across the country.26

These assertions are not without factual basis. Nations such as China and Russia have written "information manipulation and exploitation into their new military doctrine and plans."27 The CIA adds India to China and Russia as nations that have strategic information warfare capabilities.28 In Russia, for example, "[u]ltranationalist Vladimir Zhirinovsky has suggested that the computer virus could be a useful tool for Russian foreign policy."29 In China, the government announced in November 1999 the creation of a new branch of the military that would be dedicated exclusively to information warfare.30

The United States has good cause for concern. As Clarke asserts, "[m]ost of the government's computers are vulnerable to intrusion,"31 either through lack of their own security systems or through private sector vulnerabilities.32 Another complication is that a successful CNA may occur without the target's

---

26 Id. at 38; see also Todd A. Morth, Note, Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter, 30 CASE W. RES. J. INT'L L. 567, 568 (1998) (comparing information warfare capabilities to those of nuclear, chemical, and biological attacks in destructive capability but contrasting them by the ease with which they can be attained).

27 BORCHGRAVE ET AL., supra note 1, at ii; see also Dan Verton, Defense Agency, Veridian to Pinpoint Foreign Hackers, INFOWORLD (Aug. 29, 2001), available at http://www.infoworld.com/articles/hn/xml/01/08/29/010829hndefense.xml (discussing Veridian's upcoming contract with the DOD to study computer intrusions and hacks by China against DOD computers).

28 Darcy Noricks, Cyber Attacks on U.S. Security, WASH. TIMES, Apr. 20, 2000, at A19; see also Verton, supra note 27 (referring to recent DIA and CIA estimates that at least twenty countries are developing information warfare strategies specifically targeting the United States).

29 David Hoffman, Russian Touts Computer Virus as Weapon, WASH. POST, May 9, 2000, at 21.


knowledge,\(^\text{33}\) and certainly without knowledge of the damage's extent. "In fact, in most cases, the attack will already be over and the damage done by the time it is identified."\(^\text{34}\) Adding to these difficulties are the problems of identifying the perpetrators,\(^\text{35}\) determining their intent,\(^\text{36}\) affixing responsibility, and applying appropriate sanctions. Furthermore, a wide array of individuals and groups not affiliated with any national or military interests have the capacity and the will to conduct a CNA on governmental entities,\(^\text{37}\) and many groups who may not be targeting governmental entities will have that secondary effect inadvertently:\(^\text{38}\)

In contrast to the still nebulous threat from nation-states, the threat from subgroups and terrorist organizations is very real. While their goal is neither war nor destruction on a large scale, the effect of attacks from politically motivated groups are [sic] likely to be more pervasive. Their goals can be disruption, intimidation, or publication of a political message . . . .\(^\text{39}\)

In sum, "[b]ecause hacker tools are increasingly cheap, accessible, and easy to 'weaponize,' disruptive attacks can be perpetrated not only by nation-states, but also by national opposition groups, ideological radicals, terrorist organizations, and individuals."\(^\text{40}\) Given U.S. vulnerabilities, it may only be a matter of time before the United States is faced with either a terrorist-sponsored cyberspace equivalent of the September 11th attacks\(^\text{41}\) or with a preparatory cyber onslaught in a situation similar to that proposed by Unrestricted Warfare, the Chinese military manual. In such a case, what legal responses would be available to the United States? Could the United States legally take any action or must it wait for an armed attack by military forces? National leaders are unlikely to allow such a catastrophic intrusion into their


\(^{34}\) Jeffrey K. Souder, Information Operations in Homeland Computer-Network Defense, J. ELECTRONIC DEF. (Oct. 1, 2001), at http://www.jedonline.com/jedonline/default.asp?journalid=4&func=articles&page=0110j12&year=2001&month=10&doctype=features. Souder continues, "[t]his fact alone implies that planning for computer attack and defense must be quite different than that of physical attack and defense," and concludes that "[w]ithin the cyberspace, distance is nearly irrelevant, speed is almost instantaneous, and forces are able to 'arrive' with little or no warning, strike, and maintain the attack for as long as necessary to attain the objective without experiencing fatigue or injury." Id.

\(^{35}\) The problem of identifying the perpetrator of the attack is also known as "attribution" and will be discussed below.

\(^{36}\) The problem of determining the attacker's intent is also known as "characterization" and will be discussed below.

\(^{37}\) BORCHGRAVE ET AL., supra note 1, at 7.

\(^{38}\) The May 2000 "Love Bug" worm is a good example of this. See id. at 12–13.

\(^{39}\) Id. at 19–20.

\(^{40}\) Id., Executive Summary, at 1; see also Angolan Cyber-Guerrilla's Raid UNITA, AFRICA ANALYSIS, Nov. 30, 2001, at 3, available at http://www.africaanalysis.com (discussing a cyber attack against UNITA by the opposition party).

sovereignty without a response involving more than diplomatic protests. International law, moreover, should not limit their range of responses. Rather, when a nation suffers a debilitating CNA, it should rightly categorize that CNA as a use of force and be able to react in self-defense.

II. USE OF FORCE IN INTERNATIONAL LAW

Implicit in the question of whether and how a nation can respond to a CNA is whether the CNA constitutes a use of force. Under current international law, if a CNA rises to the level of a use of force, the victim nation may have a broader range of options than if it does not constitute a use of force. Therefore, it is necessary to determine exactly what constitutes a use of force and to assess how a nation may legally respond either in reaction to or in anticipation of such a use of force.42

A. Use of Force Prior to the U.N. Charter

Since the Treaty of Westphalia ended the Thirty Years War in 1648, the nation-state has been the primary actor on the international stage. As a result, one of the main forces driving the development of the use of force in international law, particularly in its early stages, has been the idea of national sovereignty:43

States conscious of their sovereignty have insistently denied, as they still deny, that other States can be judges; claiming also, by implication if not expressly, that the power of international law to control what they do by virtue of these claims diminishes in proportion with the directness and immediacy of the perceived danger to national existence.44

Despite the importance of state sovereignty, governments in the nineteenth century began to see the benefits of sacrificing some sovereignty in exchange for increased predictability. As the 1856 Declaration of Paris, one of the first such international agreements, stated, "the uncertainty of the [maritime] law and of the duties in such a matter, gives rise to differences of opinion between neutrals and belligerents which may occasion serious difficulties, and even conflicts."45 In an attempt to avoid these "difficulties," nations limited their "legal" recourses of action in resorting to force.

The trend continued with agreements such as Hague I (1899 and 1907),46 the Covenant of the League of Nations (1919),47 and the Kellogg-Briand Pact

42 Taking action in anticipation of a use of force is commonly referred to as "anticipatory self-defense" and will be discussed below.
43 GEOFFREY BEST, HUMANITY IN WARFARE 17–18 (1980).
44 Id. at 18.
46 Pacific Settlement of International Disputes (Hague I) July 29, 1899, reprinted in 1 BEVANS 230. As rewritten and repromulgated on Oct. 18, 1907, Article 1 introduced language of international dispute settlement that became the basis for similar agreements over the next century: "With a view to obviating, as far as possible, recourse to force in the relations between States, the Signatory Powers agree to use
These agreements, however, failed to prevent the conflagration of World War II. Ironically, within fourteen years of the Kellogg-Briand Pact, which renounced recourse to war, many of the participating countries had become engaged in hostilities with each other. What essentially came from these agreements was a lesson on the limitation of violence and the importance of international agreements in accomplishing that goal.49

B. The U.N. Charter and the Current Law on the Use of Force

After World War II, the leaders of the dominant world states attempted to create an international system that would promote a lasting peace. The result was the United Nations and its founding document, the U.N. Charter.50 Like the League of Nations that preceded it, the United Nations limited the legality of a nation's ability to resort to war.51 The first purpose of the United Nations, their best efforts to insure the pacific settlement of international differences.” Id. at 234. Articles 9-57 of the agreement went on to outline a voluntary system of mediation and arbitration designed to resolve disputes before nations felt it necessary to resort to the use of force. Id. at 236-43.

47 LEAGUE OF NATIONS COVENANT, reprinted in WOODROW WILSON’S CASE FOR THE LEAGUE OF NATIONS, at app. f (Hamilton Foley ed., 1969) (describing the intent, structure, and battle for the League of Nations). The preamble of the Covenant of the League of Nations states the intent of the framers: “In order to promote international cooperation and to achieve international peace and security by the acceptance of obligations not to resort to war . . . .” LEAGUE OF NATIONS COVENANT pmbl. Though no language of the Covenant made a resort to war illegal per se, it required nations to submit "any dispute likely to lead to a rupture" to arbitration or to the League Council. Id. arts. 12, 15. Further, Article 16 states:

Should any Member of the League resort to war in disregard of its covenants under Articles 12, 13, or 15, it shall ipso facto be deemed to have committed an act of war against all other Members of the League, which hereby undertake immediately to subject it to the severance of all trade or financial relations, the prohibition of all intercourse between their nationals and the nationals of the covenant-breaking State, and the prevention of all financial, commercial, or personal intercourse between the nationals of the covenant-breaking State and the nationals of any other State, whether a Member of the League or not.

It shall be the duty of the Council in such case to recommend to the several Governments concerned what effective military, naval, or air force the Members of the League shall severally contribute to the armed forces to be used to protect the covenants of the League.

Id. art. 16.

48 Kellogg-Briand Pact (1928), reprinted in 2 BEVANS 732. Articles I and II of the Treaty state:

Article I. The High Contracting Parties solemnly declare in the names of their respective peoples that they condemn recourse to war for the solution of international controversies, and renounce it as an instrument of national policy in their relations with one another.

Article II. The High Contracting Parties agree that the settlement or solution of all disputes or conflicts of whatever nature or of whatever origin they may be, which may arise among them, shall never be sought except by pacific means.

Id. at 734.


50 U.N. CHARTER, reprinted in 3 BEVANS 1153.

51 U.N. CHARTER pmbl. The preamble states:

We the peoples of the United Nations determined to save succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind . . . and for these ends to practice tolerance and live together in peace with one another as good neighbors, and to unite our strength to maintain international peace and security, and to ensure, by the acceptance of principles and the institution of methods, that armed force shall not be used, save in the common interest . . . have resolved to combine our efforts to accomplish these aims.
according to Article 1 of the U.N. Charter, is to maintain international peace and security through collective measures and to block acts of aggression or breaches of the peace. 

While Article 1 outlines the fundamental purposes of the United Nations, Article 2 addresses the principles by which the member states must pursue those purposes. Among these is Article 2(4), which limits a nation’s ability to use force unilaterally: “All 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.” This seemingly complete renunciation of force is tempered by two potential exceptions: first, a collective military action authorized by the U.N. Security Council, and, second, the longstanding international law principle of the right of self-defense. These two provisions embody current legal restraints on a nation’s decision to use or threaten force under the going ad bellum doctrine, or the law of conflict management.

C. Security Council Response

Article 39, found in Chapter VII, establishes a collective method of enforcement in response to a Charter violation by a breach of the peace, a

---

52 Id. art 1. Article 1 states:

The Purposes of the United Nations are: 1. To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace . . . .

53 Id. art. 2, para. 4.

54 The composition and functions of the Security Council are covered in Chapter V of the U.N. Charter, comprising Articles 23–32. Id. arts 23–32. The Security Council has primary responsibility for international peace and security (Article 24) as described in Chapters VI, VII, VIII, and XII, comprising Articles 33–54 and 75–85. Id. arts 33–54, 75–85.

55 Id. art. 51.

56 Article 2(7) allows for a nation to use or threaten force in “matters which are essentially within the domestic jurisdiction of any state” without U.N. intervention. Id. art. 2, para. 7. Nothing continued in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state or shall require the Members to submit such matters to settlement under the present Charter; but this principle shall not prejudice the application of enforcement measures under Chapter VII.


58 U.S. DEP’T OF STATE, CHARTER OF THE UNITED NATIONS: REPORT TO THE PRESIDENT ON THE RESULTS OF THE SAN FRANCISCO CONFERENCE BY THE CHAIRMAN OF THE UNITED STATES
threat to peace, or an act of aggression. It provides that "[t]he Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security." In other words, the U.N. Charter authorizes the Security Council to determine the nature of a nation's actions and to decide what preventive or remedial actions are appropriate. The Security Council used this power to authorize collective action against Iraq after it invaded Kuwait in 1990. By delegating this determinative power, the U.N. Charter has removed it from each individual nation except to the extent provided in Article 51 for self-defense.

D. Anticipatory Self-Defense

Article 51 is the second exception to the Article 2(4) prohibition on the threat or use of force, codifying the customary international right to use force in self-defense. It provides that "[n]othing contained in the present Charter shall impair the inherent right of individual or collective self-defense 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

DELEGATION, THE SECRETARY OF STATE 88 (1945) (describing Chapter VII as "the teeth of the United Nations") [hereinafter REPORT TO THE PRESIDENT]. The Report continues,

While the novel quality of the enforcement measures envisaged in that Chapter may attract undue public attention at the expense of other vital functions of the Organization, the fact remains that upon the confidence which member states repose in the efficacy of the measures designed to halt aggression—a confidence which may have to meet the test of successive crises—the survival of the entire Organization and of world peace itself must ultimately depend.


60 U.N. CHARTER art. 39. Article 41 states:

The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.

Id. art. 41. Article 42 states:

Should the Security 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. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations.

Id. art. 42.


62 Article 51 was originally framed with the primary intent of incorporating regional systems from Chapter VIII into the international security system, not as a means of one nation using force to preempt or respond to an attack from another nation. See REPORT TO THE PRESIDENT, supra note 58, at 107.
security." The Article therefore preserves the long-standing principle that a nation has the inherent right to defend itself. Though at times the doctrine has been used to justify aggressive actions, self-defense has been enshrined as a legitimate principle of international law and was included in the U.N. Charter precisely because the founding delegates mistrusted complete reliance on collective security.

Two principles limit the doctrine of self-defense: necessity and proportionality. Necessity is the imminent danger of an armed attack; proportionality "is the degree of force, that is reasonable in terms of intensity, duration and magnitude, required to decisively counter the hostile act or demonstration of hostile intent that constitutes the necessity part of the equation—but no more than that." Any act of self-defense must therefore be out of necessity and must be proportional to the threat against which it defends.

Incorporated in the right of self-defense is the doctrine of anticipatory self-defense. As articulated by the nineteenth century U.S. statesman and

63 U.N. CHARTER art. 51. Article 51 continues:
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.

Id. art. 51.


65 NORMAN BENTWICH & ANDREW MARTIN, A COMMENTARY ON THE CHARTER OF THE UNITED NATIONS 106 (1950) (providing the German aggression against Luxembourg and Belgium in August 1914, the Japanese aggression in Manchuria in 1931-32, and the German aggression against Poland in September 1939 as examples of the misuse of the doctrine of self-defense).

66 Id.


68 Id.


70 The quintessential statement of the right of anticipatory self-defense was espoused in 1842 by the U.S. Secretary of State, Daniel Webster, in The Caroline incident. In a letter to Henry Fox, the British Minister in Washington, D.C., Webster argued that an action by the British was not justified by anticipatory self-defense:

The statement of Secretary of State Daniel Webster on The Caroline incident in 1842 has been widely accepted and was quoted approvingly by the Nuremberg Tribunal. Webster said, with reference to the invasion of U.S. territory across the Niagara River by British forces to prevent aid to Canadian revolutionaries from The Caroline, which was loaded with arms and about to depart, that such invasion was in principle illegal, but he added "while it is admitted that exceptions growing out of the great law of self-defense do exist, those exceptions should be confined to cases in which the necessity of that self-defense is instant, overwhelming, and leaving no choice of means and no moment for deliberation, and must be limited by that necessity and kept clearly within it.

Self-Defense, 5 Whiteman DIGEST § 25, at 981–82 (citations omitted); see also Sharp, supra note 57, at 43 (discussing anticipatory self-defense under the U.N. Charter). But see Timothy Kearley, Raising the Caroline, 17 WIS. INT’L L.J. 325 (1999) for the assertion that Webster’s original meaning and the original understanding of the doctrine of anticipatory self-defense applied only to actions outside a state’s own territory. It is only since the Charter that this doctrine has been used to justify acts within a state’s own territory. Id.
Secretary of State Daniel Webster, when the necessity of self-defense is "instant, overwhelming, and [leaves] no choice of means and no moment for deliberation,"71 a nation may act preemptively to protect itself. The doctrine of anticipatory self-defense, therefore, was a clearly accepted principle of international relations prior to the U.N. Charter.72 Since the founding of the United Nations, the doctrine of anticipatory self-defense has come under close scrutiny. The reason can be found in Article 51's wording. Read literally, the trigger for a state to invoke its right of self-defense is the requirement of an "armed attack." This appears to mean that a nation must absorb an initial armed attack, in whatever form, before it can use force without prior Security Council authorization. Some scholars argue that despite the "armed attack" requirement of Article 51, the Charter did not intend to extinguish preexisting doctrine.73 Others advocate some form of anticipatory self-defense not as extensive as the pre-Charter principle, but one not requiring that an actual "armed attack" occur.74 Still others argue that Article 51 clearly requires an actual "armed attack" before the right to self-defense can be triggered and that the doctrine of anticipatory self-defense has been eviscerated.75

While scholars debate these questions, the International Court of Justice (ICJ)76 has given some indication of what it believes; because it relies on existing international law as drawn from recognized sources,77 its opinions are instructive in this unresolved area. In a recent case involving the United States and Nicaragua,78 the ICJ discussed what state actions might call for the use of force in self-defense. The case concerned U.S. actions in Honduras that Nicaragua claimed amounted to an armed attack, but that the United States claimed were made in collective self-defense of Honduras. In making its decision, the Court stated that not all uses of force amount to an armed attack,79 and not all interventions by one state into the affairs of another rise to the level of a "use of force."80 In regards to the right to the level of self-defense, however,

71 Whiteman, Self-Defense, supra note 70.
73 See, e.g., MCDouGLA & FElicIANO, supra note 72, at 235; D.W. BOWETT, SELF-DEFENCE IN INTERNATIONAL LAW 184-93 (1958); TIMOTHY L.H. MCCORMACK, SELF-DEFENSE IN INTERNATIONAL LAW 139-44 (1996).
74 YORAM DINSTEIN, WAR, AGRESSION AND SELF-DEFENCE 182-91 (2d ed. 1994) (arguing that a standard of "interceptive" self-defense is legitimate under Article 51 of the U.N. Charter. Interceptive self-defense refers to actions taken after the other side has committed itself to an armed attack.).
75 MCDouGLA & FElicIANO, supra note 72, at 232-34; Simma, supra note 72, at 675-76; LOUIS HENKEN, HOW NATIONS BEHAVE 141-45 (2d ed. 1979); Permissible and Impermissible Uses of Force, 12 Whiteman DIGEST § 1, at 48.
76 The Permanent Court of International Justice, formed in 1921 at The Hague, was succeeded by the ICJ in 1946. See also CARTER & TRIMBLE, supra note 49, at 296-97.
79 Id. at 101 (Merits).
80 Id. at 119 (Merits).
the Court held that the right is "subject to the State concerned having been the victim of an armed attack." Because anticipatory self-defense was not raised in the facts of the case, the Court did not address this issue; it is fair to assume, however, that the Court would not have allowed a more extensive right of self-defense exercised in anticipation of an attack than one exercised after an attack. Therefore, the ICJ would likely place the same requirements on the right of anticipatory self-defense, making it subject to a prior armed attack.

State practice of self-defense has also proved inconclusive. Several incidents since the U.N.'s inception have provided opportunities for states to opine on anticipatory self-defense policy; these incidents have, however, provided mixed results. For example, the U.N. Security Council unanimously condemned an Israeli attack on an Iraqi nuclear reactor in 1981. Nevertheless, the act was likely condemned because the circumstances did not meet the "imminent" requirement of self-defense, rather than any sort of denial of the anticipatory self-defense doctrine. The United States took part in that condemnation vote, but the United States clearly believes the doctrine of anticipatory self-defense is consistent with the U.N. Charter and will apply it as deemed necessary. For example, the U.S. bombing of Libya in 1986 was justified by President Ronald Reagan as being "fully consistent with Article 51." Therefore, it seems that the ambiguity regarding anticipatory self-defense has not prevented those nations wishing to adopt it from doing so.

As an alternative to anticipatory self-defense, the ICJ provided that a state might take proportionate countermeasures in response to intervention amounting to a use of force but not rising to the level of an armed attack. Referring to the Nicaragua case, the ICJ enumerated three conditions to justify proportionate countermeasures. First, the action must be taken in response to a previous international wrongful act of another state, and it must be directed against that state. Second, the injured state must have called upon the offending state to discontinue its wrongful conduct or to make reparation for it. Third, the countermeasure must be commensurate with the injury suffered, taking into account the rights in question.

81 Id. at 103 (Merits).
82 Id. But see id. at 347 (Schwebel, dissenting).
84 Id. at 161.
85 OFFICE OF THE GENERAL COUNSEL, DEP'T OF DEFENSE, AN ASSESSMENT OF LEGAL ISSUES IN INFORMATION OPERATIONS 15 (2d ed. 1999) [hereinafter DOD OGC].
86 MCCORMACK, supra note 73, at 229.
87 Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 94, 127 (June 27) (Merits). The Court does not describe or further explain what these proportional countermeasures might include. It merely states that such measures would be permissible in response to a use of force short of armed attack. Id.
It follows from this three-part analysis that if the right to anticipatory self-defense does not arise until the aggressing nation is on the verge of armed attack, and if a CNA is always deemed to fall below that threshold, a threatened nation must rely on the use of countermeasures that may only come in response to a prior act. In other words, unless a CNA equates to an armed attack, a nation will not have the right of self-defense. Rather, the victim nation will have to meet the ICJ’s conditions for proportional countermeasures, including the requirement to put the aggressor state on notice and give it the opportunity to cease action and make reparations. In the age of instantaneous computer lethality, this approach is unresponsive and provides insufficient protection from potential CNA threats. To illustrate the shortcomings of this approach, the following section will discuss the various levels of CNAs that constitute either an armed attack or a use of force.

III. CNA AS A USE OF FORCE

The question of whether a CNA constitutes a use of force or an armed attack is significant in determining what responses are legal and effective under international law. Though the ICJ used the Article 51 term “armed attack” in determining the conditions necessary to trigger the right to self-defense, the Court did not decide the U.S.-Nicaragua case under the U.N. Charter. Rather, it relied on customary international law and held that the pre-U.N. right of self-defense was not completely subsumed or supervened by the Charter. Furthermore, the Court’s unwillingness to address the issue of anticipatory self-defense leaves some room for states to invoke anticipatory self-defense in circumstances other than those contemplated by the Nicaragua decision—for example, in cases of a CNA by a non-state actor. Otherwise, if the right of self-defense does not accrue until an armed attack has occurred, then little meaning is left in the doctrine of anticipatory self-defense with regard to CNAs. Any strength left to the doctrine rests upon a narrow definition of “armed attack” and upon what preparatory uses of force actually fit within that very restricted meaning.

say so, the Court in that case strongly suggested that a victim of an illegal act involving the use of force could legally respond with forceful countermeasures); D.G. Stephens, The Impact of the 1982 Law of the Sea Convention on the Conduct of Peacetime Naval/Military Operations, 29 CAL. W. INT’L L.J. 283, 303-04 (1999) (stating that the right to use force as a countermeasure was implicit in the ICJ’s opinion in the Nicaragua case). Compare Oscar Schachter, United Nations Law, 88 AM. J. INT’L L. 1, 15 (1994), where the author states:

The term “countermeasures” has come to be used for self-help action in place of the older terms “reprisal” and “retorsion.” But it is still relevant to distinguish between countermeasures that would be illegal if not for the prior illegal act of the state against which they are directed (i.e., reprisals) and countermeasures that a state could legally take against any state irrespective of that state’s conduct (retorsion). Both may be regarded as sanctions against violations. Reprisals are generally permitted if they do not involve use of force contrary to the Charter and if they are directed to obtaining redress for the wrong committed.

Id.

90 Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 94, 96-97 (June 27) (Merits) (discussing the Court’s decision to apply customary international law rather than multilateral treaties such as the U.N. Charter, based on objections by the United States).

91 Id. at 94 (Merits).
A CNA can be characterized in three ways: first, as an action that lies below the threshold of use of force; second, as an action that is equivalent to a use of force but is short of an armed attack; or, third, as an action that equates to an armed attack. Weapon systems or more traditional means of attack can be easily classified into one of these categories. A large-scale cruise missile launch, for example, would be classified as an “armed attack.” Contrariwise, diplomatic sanctions or condemnatory speeches fall below the use of force threshold. The classification system is, however, not as successful in classifying CNAs, which, as noted, can occur in many ways.92 A CNA may be as benign as preventing a website from functioning properly or as serious as hampering public transportation and causing civilian deaths:

[A CNA] challenges the prevailing paradigm, for its consequences cannot easily be placed in a particular area along the community values threat continuum. 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). It can affect economic, social, mental, and physical well-being, either directly or indirectly, and its potential scope grows almost daily, being capable of targeting everything from individual persons or objects to entire societies.93

Because of the broad spectrum of attacks, it is unreasonable to assume that a CNA will always meet the level of a use of force under the U.N. Charter. Conversely, it is equally unreasonable to argue that because a CNA does not physically destroy the object of attack in the traditional sense, it can never amount to a use of force or an armed attack. Therefore, any theory of CNA classification must allow for different levels of CNA to fit into all three categories. This problem is complicated by the few known examples of CNAs, which make it difficult to assess what states will ultimately consider appropriate when dealing with CNAs and the use of force.94


Both the Charter and customary conceptions of international law with regard to use of the military instrument rested on a set of inherited assumptions about how military conflict is conducted: conflict is territorial, between organized communities; conducted by certain types of specialists in violence or "regular forces" who are clearly identified; they concentrate their efforts against each other in a war zone; the conflict itself is preceded by formal notification; suspended by some formal arrangement, and terminated in an explicit and often ceremonialized fashion.

Id., quoted in Richard W. Aldrich, How Do You Know You Are at War in the Information Age?, 22 HOUS. J. INT'L L. 223, 234 (2000) (arguing that the underlying assumptions that were the basis for the rules on the use of force may not be sufficient to fit the technological warfare possible today).

93 Schmitt, Normative Framework, supra note 33, at 912.

94 State practice is one of the ways customary international law is established. For example, in the statute of the Permanent Court of International Justice, the court is allowed to look at the practice of states. See Source: Custom, I Whiteman DIGEST § 6, at 75.

It is not possible for the Court to apply a custom; instead, it can observe the general practice of States, and if it finds that such practice is due to a conception that the law requires it, it may
Recent scholarly writing has produced at least two prominent theories concerning the level of CNAs that will amount to a use of force under the U.N. Charter. Walter Gary Sharp, Sr. argues that threats to use force may rise to the level of an unlawful use of force in violation of Article 2(4), but may not trigger a nation’s Article 51 right to anticipatory self-defense. On the other hand, at some point a threat to use force that is short of actual use demonstrates hostile intent and triggers a nation’s right to anticipatory self-defense. Sharp also argues that “the Article 2(4) prohibition on the use of force also covers ‘physical force of a non-military nature’ committed by any state agency,” and that such nonmilitary actions “may produce the effects of an armed attack prompting the right of self-defense laid down in [Article] 51 of the U.N. Charter.” Sharp applies this same paradigm to CNAs.

Sharp has urged that “any computer network attack [conducted by a state actor] that intentionally causes any destructive effect within the sovereign territory of another state is an unlawful use of force that may constitute an armed attack prompting the right to self-defense” under Article 51 of the U.N. Charter. In coming to his conclusion, Sharp draws an analogy between a CNA and the unlawful penetration of a nation’s airspace by aircraft designed to gather sensitive information. He concludes that, although merely penetrating a nation’s cyberspace may be in violation of domestic law, it is not a use of force. Furthermore, this use of cyberspace to conduct computer

---

95. Statements of scholars can also provide a basis for international law, particularly when the specific area of law is not developed enough to evidence much state practice and few, if any, international agreements exist in the area. See International Law: General Nature, 1 Hackworth DIGEST § 1, at 1.

96. SHARP, supra note 57, at 91.

97. Id. at 92.

98. Id. at 226 (quoting CHAIRMAN, THE JOINT CHIEFS OF STAFF INSTRUCTION 3121.01, STANDING RULES OF ENGAGEMENT FOR U.S. FORCES, encl. A, paras. 5e, 5f (Oct. 1, 1994, amended Dec. 22, 1994) (discussing the U.S. military’s definitions of hostile intent and hostile act)). These 1994 rules were replaced on Jan. 15, 2000 by CHAIRMAN, JOINT CHIEFS OF STAFF INSTRUCTION 3121.01A, STANDING RULES OF ENGAGEMENT FOR U.S. FORCES (2000) [hereinafter INSTRUCTION 3121.01A].

99. SHARP, supra note 57, at 93.

100. Id. at 101.

101. Id. (quoting Simma, supra note 72, at 113) (listing “cross frontier expulsion of populations, the diversion of a river by an up-stream state, the release of large quantities of water down a valley, and the spreading of fire across a frontier” as examples of nonmilitary physical force that would amount to a use of force).

102. Id. at 133.

103. Id. at 126.

104. Id. at 127–28.
Espionage is legal under international law. Depending on the target system of the computer espionage and the results, however, the act may rise to an unlawful violation of Article 2(4) and allow the victim nation to respond in anticipatory self-defense.

If, for example, the target of the computer espionage is one of the "sensitive systems that are critical to a state's vital national interests," a presumption arises that the state has the right to use necessary and proportional force in anticipatory self-defense. For other, nonpresumptive computer networks, Sharp advocates the application of hostile intent as a basis for the victim nation's response. In other words, if the intruder's actions demonstrate hostile intent, the victim nation may consider itself the object of a use of force, and, depending on the scope, duration, and intensity of the attack, the victim nation may consider such actions an armed attack.

This view is not without its skeptics. At least one prominent scholar, Michael N. Schmitt, believes that economic or political coercion does not amount to a threat or use of force, though he agrees that a use of force is not confined to traditional "physical or kinetic force applied by conventional weaponry." Schmitt proposes a more restricted view of self-defense:

[Self-defense should be] limited to operations which are de facto armed attacks, or imminently preparatory thereto. The net result is a limitation on both state resort to CNA techniques which might threaten global stability and on individual responses which might themselves prove destabilizing.

---

105 Id. at 148 (quoting THE JOINT CHIEFS OF STAFF, JOINT PUB. NO. 1-02, DICTIONARY OF MILITARY AND ASSOCIATED TERMS 174 (1998) [hereinafter JOINT PUB. 1-02] (defining espionage as "[t]he act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense of a state with an intent, or reason to believe, that the information may be used to the injury of that state or to the advantage of any foreign nation").

106 SHARP, supra note 57, at 129.


108 Id. at 129.

109 Id. at 132.

110 For example, though a CNA that causes a single train crash within a victim state would constitute an unlawful use of force, only a series of incidents or one major incident such as causing the nation's stock exchange to crash would rise to the level of an armed attack. Id. at 117.


112 Schmitt, Normative Framework, supra note 33, at 908.

113 Id.

114 Id. at 886.
Schmitt therefore focuses on the consequences of the attack rather than on the object of the attack or on the intentions of the attacker. Exceptions are cases where the attacker “specifically intends to cause physical damage to tangible objects or injury to human beings,” in which case Schmitt would view the use of armed force legal under the U.N. Charter. In cases where the attacker lacks such intent, Schmitt looks to the consequences of the attack. This means that a CNA not amounting to an armed attack would still qualify as a use of force if its effects are similar to those that would result from a similar attack with armed force.

Like Sharp, Schmitt also advocates anticipatory self-defense, but only if three factors are present:

1. The CNA is part of an overall operation culminating in armed attack;
2. The CNA is an irrevocable step in an imminent (near-term) and probably unavoidable attack; and
3. The defender is reacting in advance of the attack itself during the last possible window of opportunity available to effectively counter the attack.

He cautions, however, that the use of force in self-defense must be against the overall armed attack, not merely in response to the CNA. This is consistent with his conception of CNA as a political means to harmful consequences rather than as a harmful end in itself.

Therefore, the two authors differ primarily in their determination of the point at which the justification for self-defense ripens. For example, Sharp

---

115 Id. at 911; see also DOD OGC, supra note 85, at 14 (stating that the consequences of a CNA are likely more important than the methods used); Michael N. Schmitt, Bellum Americanum: The U.S. View of Twenty-First Century War and Its Possible Implications for the Law of Armed Conflict, 19 Mich. J. Int'l L. 1051, 1071-72 (1998) [hereinafter Schmitt, Bellum Americanum] (discussing the difference in consequence between a devastating economic embargo which would not be considered a use of force or armed attack and a minor border incursion that may be considered a use of force and possibly an armed attack).

116 Schmitt, Normative Framework, supra note 33, at 934.

117 Id. at 935. Schmitt’s analysis proceeds as follows:

2) If it is not armed force, is the CNA nevertheless a use of force as contemplated in the U.N. Charter? It is if the nature of its consequences track those consequence commonalities which characterize armed force.

3) If the CNA is a use of force (armed or otherwise), is that force applied consistent with Chapter VII, the principle of self-defense, or operational code norms permitting its use in the attendant circumstances?

a) If so, the operation is likely to be judged legitimate.

b) If not and the operation constitutes a use of armed force, the CNA will violate Article 2(4), as well as the customary international law prohibition on the use of force.

c) If not and the operation constitutes a use of force, but not armed force, the CNA will violate Article 2(4).

4) If the CNA does not rise to the level of the use of force, is there another prohibition in international law that would preclude its use? The most likely candidate, albeit not the only one, would be the prohibition on intervening in the affairs of other States.

Id. Schmitt uses the term “operational code” to refer to actions that do not fall within the prescribed limitations of the Charter, but that are accepted nonetheless. Id. at 902-03.

118 Id. at 932-33.

119 “Note that it is not the CNA that is actually being defended against, but instead the overall armed attack, complete with its information operation component.” Id. at 933.
would classify a CNA that successfully penetrates a sensitive computer system and plants a virus designed to erase data at some future point as a use of force amounting to an armed attack. In contrast, Schmitt would classify it as such only if the data erasure would result in some consequence characteristic of an armed attack. Furthermore, unless the act met the three factors required for anticipatory self-defense, Schmitt would condemn preemptory action.

A recent publication from the Department of Defense Office of General Counsel (DOD OGC), An Assessment of International Legal Issues in Information Operations, takes a middle approach. The DOD OGC agrees with Schmitt that the consequences of the attack are more important than the means of the attack:

"If a coordinated computer network attack shuts down a nation's air traffic control system along with its banking and financial systems and public utilities, and opens the floodgates of several dams resulting in general flooding that causes widespread civilian deaths and property damage, it may well be that no one would challenge the victim nation if it concluded that it was a victim of an armed attack, or of an act equivalent to an armed attack."

Notably, the DOD OGC does not explain how it would view a limited CNA (e.g., mere shutting down of the banking and financial institutions) rather than a more sophisticated CNA that also causes physical destruction.

Despite the differences, all three views agree that, at some level, the nature of the target is vital in determining whether a CNA rises to the level of a use of force or an armed attack. Sharp distinguishes targets that are critical to vital national interests as deserving special protection. Targeting these specific systems would amount to a use of force against which a nation could exercise self-defense. To illustrate the nature of such a sensitive system, Sharp looks to Executive Order 13,010, which was signed by President Bill Clinton in 1996 and which defines, at least in broad terms, the computer networks of vital importance to national security:

Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government.

In addition, the Order specifically highlights the vulnerabilities of these critical infrastructures. "Threats to these critical infrastructures fall into two categories: physical threats to tangible property ("physical threats"), and threats of electronic, radio-frequency, or computer-based attacks on the

---

120 DOD OGC, supra note 85.

121 Id. at 16.

122 Exec. Order No. 13,010, supra note 107.

123 Id.
information or communications components that control critical infrastructures ('cyber threats')."

Though the 1996 Order does not say what the response to such attacks would be, it does at least single out specific infrastructures and computer networks as "vital" to U.S. national security.

President George W. Bush has reiterated Clinton's focus in Executive Order 13,231 ("Critical Infrastructure Protection in the Information Age"), which was signed on October 16, 2001 and which states that "[p]rotection of [critical infrastructure] systems is essential to the telecommunications, energy, financial services, manufacturing, water, transportation, health care, and emergency services sectors." Bush also commits the United States to act when such infrastructures are threatened:

It is the policy of the United States to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible.

In addition, the October 2001 Order charges agency heads with implementing, "within available appropriations . . . [c]ost-effective security [and with making it] an integral part of government information systems, especially those critical systems that support the national security and other essential government programs." The Order goes on to establish the National Infrastructure Advisory Council (NIAC), "which shall provide the President advice on the security of information systems for critical infrastructure supporting other sectors of the economy: banking and finance, transportation, energy, manufacturing, and emergency government services."

---

124 Id.
126 Id.
127 Id. at 53,064.
128 Id. at 53,069. As mentioned previously, President Bush has also appointed Richard Clarke, see supra notes 23–26 and accompanying text (quoting Clarke on computer security), as his special advisor on cyberspace security. Scott Lindlaw, Officials Named for Anti-Terrorism Fight, THE ADVOCATE (Baton Rouge, La.), Oct. 1, 2001, at 11-A. The White House Office of Cyberspace Security has made the creation of "an analysis center that would help government target the most vulnerable points in the nation's critical infrastructure" one of its top priorities. Bara Vaida, Cybersecurity Chief Pushes Early-Warning System, NAT'L JOURNAL'S TECH DAILY, Nov. 26, 2001, available at http://www.govexec.com/dailyfed/1101/112601td2.htm. Mr. Clarke has identified ten goals on which the Office of Cyberspace Security is currently working:

1. He and his team in late spring or early summer will release a national cybersecurity strategy worked out with the private sector, "not a table-top book" but one "in Internet time, living in cyberspace," that will be updated as needed. (2) The FY 2003 budget proposes 8% of IT funds be used for security, although Clarke admitted "we cannot cure many problems in computer networks in one year." (3) Clarke will continue to encourage Internet leaders such as Microsoft's Bill Gates, Oracle's Larry Ellison and Cisco System's John Chambers to focus on security, as those individuals have promised. (4) His team will work with Tier One ISPs to improve Internet security. (5) Scholarships for IT security will be funded in exchange for commitments to work for the federal govt. (6) The govt. and the private sector will work to develop a cyberintelligence warning network "to share information in real time."
While Bush, like Clinton before him, did not enunciate specific actions that he would authorize in response to such an attack, the link he draws between critical infrastructure systems and national security reflects the importance of these systems. He calls for preventive measures and uses words such as "vital" and "essential," all of which draw attention to the significance of an attack on such systems. If these Executive Orders are a pronouncement of U.S. state practice on the issue, they may be precursors of a trend among nations.

Taking into account these recent Executive Orders, it appears that while Schmitt has the more accurate view of the current state of international law, Sharp has the more forward-looking view. Schmitt's opinion that economic and political coercion do not amount to a use of force is true under the prevailing view of international law. However, it may not be the state of the law in five years, as nations try to find ways within the U.N. Charter to defend themselves from ever-increasing technological vulnerabilities, such as those hinted at in the Executive Orders. Given the continual escalation of reported CNAs, Schmitt believes that a narrow construction of CNA as a use of force may be insupportable because it will act as a stringent limitation on a nation's likelihood of resorting to such measures. In fact, restraining a nation's ability to respond aggressively to a CNA will, if anything, encourage rogue nations, terrorist organizations, and individuals to commit increasingly severe attacks—precisely to ascertain the point at which a CNA will produce a forceful response. Contrariwise, Sharp argues that CNAs that intentionally cause destruction constitute a use of force, a scenario that does not correspond to the current state of international law. His approach may, however, be more effective in deterring a nation's, terrorist's, or individual's resort to CNAs. Lowering the threshold at which CNAs constitute a use of force or armed attack allows more flexibility in anticipatory self-defense. If an attacker knows that a CNA may or is likely to elicit a proportional response from the victim nation, the attacker may be deterred effectively.

possibility of a separate network such as GovNet will continue to be examined, an effort Clarke said was being researched now by 167 companies. (8) A national infrastructure modeling center would be developed to predict and cope with future attacks. (9) Homes and small businesses would be encouraged to increase cybersecurity. (10) The Commerce Dept.'s critical infrastructure efforts would work hand-in-hand with the FBI's National Infrastructure Protection Center (NIPC).


129 See Alan Goldstein, Ashcroft Warns About Cyberattacks; Attorney General Calls For More Protection of Critical Infrastructure, DALLAS MORNING NEWS, Feb. 13, 2002, at 1D (Business Section) ("U.S. Attorney General John Ashcroft warned Tuesday that potential terrorist invasions of computer networks could be just as dangerous as attacks on physical places, saying that more needs to be done to protect the nation's so-called critical infrastructure.").

130 But see Winkler Says Gov't Ignored Cyberattack Wake-up Calls, COMM. DAILY, Mar. 1, 2002, LEXIS, Nexis Library, CURNWS File (quoting Ira Winkler, chief security strategist for Hewlett-Packard, who condemns the government's inaction and lack of real response to warnings over the past five years saying, "[t]here have been no lessons learned or applied by government . . . any of the practical lessons learned would have prevented a lot of these problems").

131 Simma, supra note 72, at 112 (arguing that Articles 2(4) and 51 were not intended to proscribe political or economic coercion); see also SHARP, supra note 57, at 99–109.
Regardless of whether current law would classify a CNA as a use of force or an armed attack, a nation must have the right to protect itself against debilitating external threats. Therefore, the law should evolve to recognize a nation's inherent right of self-defense, including anticipatory self-defense, against a CNA focused on critical national infrastructure, even if that CNA does not constitute an armed attack.

IV. RESPONDING TO CNA IN ANTICIPATORY SELF-DEFENSE

State practice will eventually elucidate the CNA levels that constitute uses of force and armed attacks that would allow an action in anticipatory self-defense. Waiting for the development of international law—to see “how the doctrines of self-defense and countermeasures will be applied to computer network attacks,” as suggested by the DOD OGC’s paper—is, however, a risky and irresponsible approach to national security. For example, the recognition of the significant risks posed will likely drive the United States, the most technologically advanced nation in the world, to take the lead in establishing state practice in an effort to push the development of international law. To do so, the United States must establish a domestic practice of protecting its critical national infrastructure, as designated in Executive Orders 13,010 and 13,231, by applying proportional force in response to or in anticipation of a CNA.

In considering appropriate proportional responses to a CNA, it is important to note the number of different options available. No requirement exists that

132 DOD OGC, supra note 85, at 23.

133 Id. Though a detailed interpretation on the current state of the law, the DOD OGC paper makes no attempt to put forward any theory on how to handle this difficult area, or even put potential offenders on notice that the United States views certain acts as violations of its sovereignty and potential uses of force.

134 The USA Patriot Act of 2001, passed in response to the September 11, 2001 terrorist acts, expands domestic legal options in the area of CND, but does not go far enough, particularly to protect critical national infrastructure. USA Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 1394 (2001). Pertinent provisions of the Act include: § 202, which adds felony violations of the Computer Fraud and Abuse Act to the list of offenses that support a voice wiretap; § 203b, which encourages sharing of information between all federal agencies; § 210, which expands the coverage of a subpoena for electronic evidence; § 211, which brings internet services within the ECPA trap and trace rules; § 214, which modifies the FISA pen register, trap and trace requirements to replace “agent of a foreign power” with a showing that the register or trap and trace is relevant to an investigation to protect against international terrorism; § 216, which expands generally pen register, trap and trace authority; § 217, which allows victims of computer attacks to authorize system monitoring; § 218, which makes obtaining foreign intelligence “a significant purpose” rather than “the purpose” of the search for obtaining a warrant; § 219, which authorizes single-jurisdiction search warrants in any district where terrorist acts may have occurred; § 220 which allows nationwide search warrants for email; § 377 which provides extraterritorial jurisdiction for certain computer data theft cases; and § 1016, which creates the National Infrastructure Simulation and Analysis Center (NISAC) and authorizes $20 million for the Defense Threat Reduction Agency. Id.

135 This Article will consider only responses that amount to a use of force and can be accomplished in a relatively quick amount of time. It will not discuss other potential responses such as diplomatic measures or sanctions, extradition of the perpetrator, and other proposed and current remedies. As discussed above, in the case of critical national infrastructure protection, these remedies take too long and will not provide sufficient protection for critical systems.
the response be done in a manner similar to the attack, only that it be done proportionally. In other words, a nation may respond to an attack with a similar CNA or with kinetic weapons, such as bombs, so long as the response is proportional. Nevertheless, while physically bombing the hacking computers and their owners is legal, it is not necessarily the preferred method of response; such a response is almost certain to be construed as an "armed attack" and may lead to escalation. The place to begin is instead in the area of CND—computer network defense.

Two types of CND safeguard computers and networks from a CNA: passive measures and active measures. Passive measures include encryption, firewalls, and automated detection. Such measures are most effective when used in combination to form a "layered" security system. ForeScout's "ActiveResponse" technology could be part of such a system. ForeScout advertises its system as being capable of performing a perimeter defense and repelling would-be attackers while tagging attackers and immediately blocking them if they try to return to the network. International law is clear in regard to passive measures: every nation has the right to protect its computer systems by such means, just as it would its own airspace or territory.

---

136 Grunawalt, supra note 67, at 251.

In [information warfare, the attacker] would be a combatant and subject to proportional response. In fact, if the target of her attack did not have the means [sic] respond with his own [information warfare] measures, he could reasonably bomb the building in which she is believed to be sitting—again a proportional response but one that returns kinetic destruction for that created by electronic means.

Id.

138 “CND is the mission to defend computer systems and networks from unauthorized activity and other activity, which degrade mission performance and adversely impact survivability (e.g., disruption, denial, degradation, destruction, or exploitation).” CHAIRMAN, THE JOINT CHIEFS OF STAFF INSTRUCTION 6510.01C, INFORMATION ASSURANCE AND COMPUTER NETWORK DEFENSE, encl. A, para. 1(a) (May 1, 2001). This mission is to be accomplished by “employing communications, law enforcement, counterintelligence, and Intelligence Community capabilities in response to specific or potential threats” (emphasis added). Id. The inclusion of defense against "potential threats" is another clear statement of the United States' commitment to apply anticipatory self-defense in the area of CNO.

139 Encryption is the process of producing a scrambled ciphertext that can only be unscrambled by someone who has the secret key or decryption. DENNING, supra note 2, at 286.

140 “A firewall is a network monitor or collection of monitors placed between an organization's internal network and the Internet or between two local area networks . . . . A firewall is essentially a guarded gateway between two networks.” Id. at 353.

141 Automated detection is the process of programming computers to "scan computer records or on-line computer activity for patterns that indicate or suggest the presence of unauthorized activity." Id. at 361.


144 DOD OGC, supra note 85, at 18.
Active means of defense, on the other hand, raise more serious issues.\textsuperscript{145} Specific capabilities are not only beyond the scope of this paper, but also are mostly classified.\textsuperscript{146} Nevertheless, active responses may involve some in-kind rejoinder or "hack-back" feature, either reflecting similar damage back to the sender or causing some other responsive action.\textsuperscript{147} These measures may be employed automatically, but usually only after the passive defensive measures are penetrated.\textsuperscript{148} The "Blitzkrieg" is such a system, designed to detect and immediately respond to malicious intruders. Its creator claims that the military version "initiates destructive, virus-type attacks against an intruder's machine."\textsuperscript{149} The capacity to automatically trace a malicious signal back to its origin and respond with digital retribution is likely to be already in existence or will be in the future.\textsuperscript{150}

Embracing an active measures policy poses additional difficulties. Any automatic response must be tailored to meet three longstanding limitations under the law governing the use of force: (1) attribution of the attack, (2) characterization of the attack, and (3) inviolability of neutral nations. These traditional limitations on the application of force present potentially fatal constraints on acceptance of such a policy. However, in this technologically advanced era in which a simple keystroke can have an immediate lethal impact, leaving no time for other currently acceptable defensive measures,\textsuperscript{151} the law must evolve to allow a nation to defend itself effectively.\textsuperscript{152}

\textsuperscript{145} Aldrich, \textit{supra} note 92, 258–60 (stating that the Department of Justice is opposed to an active computer network defense system because of potential difficulties inherent in controlling such a response and because it believes such a system would violate the Computer Fraud and Abuse Act; and, urging national security exemptions to these laws to facilitate an adequate defense against information warfare).


\textsuperscript{147} \textit{DENNING}, \textit{supra} note 2, at 392.

\textsuperscript{148} William B. Scott, \textit{Network Security Still the ‘Wild West,'} \textit{AVIATION WK. & SPACE TECH.}, Feb. 26, 2001, at 62 (quoting a high-level Pentagon official as saying the government has an "immediate kill" tactic already in place to protect national "crown jewels" against network intrusions).

\textsuperscript{149} \textit{DENNING}, \textit{supra} note 2, at 393.

\textsuperscript{150} Prem Kumar, \textit{Tactics to Combat Cyber-Attacks}, \textit{BUS. LINE}, Jan. 9, 2002, LEXIS, Nexis Library, CURNWS File, where the author states:

With the rapid rise in the attacks on military computers, the guardians of the Pentagon information system want to look beyond the passive set-up of firewalls, sensors and computer experts. According to the journal Defense News, there is a proposal to deploy Active Network Defense, which "will track down hackers with techniques that trace the origin of the attack."

\textit{Id.}

\textsuperscript{151} Walker, \textit{supra} note 2, at 1103.

A. Attribution of the Attack

The issue of attribution turns on whether a victim nation can lawfully launch a response without knowing the identity of the attacker. Consider, for example, the case of a network administrator sitting at his computer somewhere in the United States. He suddenly detects an intrusive and potentially life-threatening CNA on a sensitive computer network, but he does not know the identity or origin of the attacker. The attacker could be a recreational hacker, a terrorist, or a foreign military member intent on destroying U.S. property and killing U.S. citizens.\(^{153}\) The requirement to attribute an attack before responding is likely to be a time-consuming process,\(^{154}\) a luxury unavailable in the cyber attack era.\(^{155}\) Because a lethal electronic signal can be sent in the time it takes to hit a computer key, there is no time both to contain damage and to identify the perpetrator.\(^{156}\) As a general principle, therefore, the requirement to attribute an attack before responding presents a significant gap in a nation’s ability to defend itself.

The problem of identifying attackers is linked to the fact that most attacks come from individuals, rather than states or state-sponsored organizations. The U.N. Charter’s prohibition on the threat or use of force is binding on all member states and is held to be customary international law by the General Assembly\(^{157}\) and the ICJ.\(^{158}\) However, the preclusion generally applies only to states and not to individuals.\(^{159}\) States are therefore prevented from threatening or using force against each other; similar acts by individuals, on the other hand,

\(^{153}\) BORCHGRAVE ET AL., supra note 1, at 3.

Understanding the distinctions between attacks and motives, and improving our nation’s ability to provide fast and accurate assessments of the nature of both the attacks and their perpetrators, are a core part of the problem at hand. \([B]oth\) the likely criminal entities and the damage they seek to inflict become more difficult to identify, quantify, and warn against. It is increasingly complicated to distinguish between a national security threat, criminal activity, and malicious but low-level disruption.


\([I]\)t would be unreasonable to preclude the victim of techno-violence from redress, based upon a doctrinaire determination that the threat of further destructive intrusions into a critical system is no longer imminent, when the perpetrator’s own actions have precluded immediate identification.

\(^{155}\) Id.

\(^{156}\) Id.

\(^{157}\) Souder, supra note 34. \("[I]\)t is possible to predict that, in many cases, attribution for the attack will not be possible."

\(^{158}\) BORCHGRAVE ET AL., supra note 1, at 46 (arguing that a passive response “undermines efforts geared at identifying attackers and adopting deterrent measures toward future hostile acts”).


\(^{159}\) Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 94 (June 27) (Merits).

\(^{159}\) Aldrich, supra note 92, at 235–36.
are generally dealt with through domestic criminal laws. The result is that a target nation will not know what avenues to pursue in response to attack until it discovers the identity of the perpetrator, a potentially costly and time-consuming process. Currently, only a few occurrences of state-on-state CNA have been reported, and these instances have been relatively benign.

160 DOD OGC, supra note 85, at 2 (noting that exceptions to this include war crimes, genocide, crimes against humanity, and crimes against peace); see also Ann Roosevelt, Computer Crime Against the Army Doesn't Pay, DEF. WK., Dec. 3, 2001, available at www.kingpublishing.com (password required) (copy on file with the author) (stating that between March 1, 2000 and October 11, 2000, the Army initiated fifty felony criminal investigations concerning intrusions into Army computer networks).

161 During armed conflict, the law of war prohibits targeting attacks on civilians unless specific criteria are met. As stated in the preamble to the 1868 Declaration of St. Petersburg, "the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy." See Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, Dec. 12, 1977, 16 I.L.M. 1391, 1442 (1977) (hereinafter Protocol Additional). The United States recognizes portions of the Protocol Additional as customary international law. Michael J. Matheson, The United States Position on the Relation of Customary Law to the 1977 Protocols Additional to the 1949 Geneva Conventions, 2 AM. U. INT'L L. & POL'Y 419, 421 (1987).

162 Oliver August, Cyberforce Threatens Taiwan, LONDON TIMES, Mar. 8, 2000, available at http://ebird.dtic.mil/Mar2000/e20000308cyberforce.htm (discussing anticipated attacks on Taiwan from China during the upcoming elections); John J. Stanton, Rules of Cyber War Baffle U.S. Government Agencies, NAT'L DEF., Feb. 2000, at 29 (discussing the cyber attack on Taiwan causing a nationwide blackout and subsequent crash of bank teller machines thought to have been caused by Chinese state-sponsored computer hacks); Warren P. Strobel et al., A Glimpse of Cyberwarfare, U.S. NEWS & WORLD REPORT, Mar. 13, 2000, at 32; see also Jim Bronskill, Crippling Cyberattack in 10 years: CSIS: Russia, China, India, Cuba Actively Advancing Cyberwar Capability, OTTAWA CITIZEN, July 18, 2001, at A3 (putting the time frame for a cyber attack at within ten years); cf. Robert Wall & David A. Fulghum, Secrecy Shrouds Computer War Threat, AVIATION WK. & SPACE TECH., Feb. 26, 2001, at 56 (quoting an Air Force general who states, "Beginning in 2005, the probability of a cyber attack using state-sponsored capability gets very high").

The most noted potentially state-sponsored attack that the government has divulged originates from Russia and has been termed Moonlight Maze. The attack started in 1998 and has been traced to seven Russian internet addresses. James Adams, writing in the May/June 2001 issue of Foreign Affairs, states "[d]espite all the investigative effort, the United States still does not know who is behind the attacks, what additional information has been taken and why, to what extent the public and private sectors have been penetrated, and what else has been left behind that could still damage the vulnerable networks." James Adams, Virtual Defense, FOREIGN AFFAIRS, May/June 2001, at 100.
vast majority of known attacks are instead from recreational hackers, who are significantly harder to track than state organizations.163

Even if the capability existed to determine the location of an attacking computer, it would not remove all obstacles to legitimizing a response. No method exists of determining whether the individual at the other end of the attack is a government agent.164 The attacker, in fact, may have gone to great measures to hide his identity.165 Though many hackers boast about their hacking prowess by leaving visible signs or signatures in their wake, this seldom is the case in national security networks hacks.166 This is also true when the attack is aimed at stealing secret or protected information, as was the case in the 2000 Microsoft hack.

Due to the potential threats involved, the staggering difficulties in quickly identifying attackers must not prevent a nation from being able to respond in self-defense. Rather, the law should permit an active response based on the target of the attack, regardless of the attacker’s identity.167 Schmitt’s position reflects this idea, arguing,

[If] twenty-first-century national security threats are to come from non-state actors, then the law governing the resort to force is bound to evolve in a way that permits an effective defense against them; this will necessitate either blurring the state/non-state actor distinction or

163 BORCHGRAVE ET AL., supra note 1, at 20; SHARP, supra note 57, at 22. It is also important to note that President Clinton determined that all such intrusions, even into critical national infrastructure, should initially be considered a law enforcement issue. Presidential Decision Directive 63, Critical Infrastructure Protection, at Annex A (May 22, 1998), available at http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

164 On the other hand, once the origin of the attack becomes known, much more severe measures could be appropriate. See DOD OGC, supra note 85, at 15 (arguing that though the response must be proportional, it need not use the same means as the attacker).

165 Schmitt, Normative Framework, supra note 33, at 892.

166 Sirak, supra note 4, at 24.

167 See, e.g., Shulman, supra note 137, at 956 (arguing that during armed conflict, even a protected person conducting a lethal CNA would lose her status and become the legitimate target of a response). Shulman states:

The person launching a computer virus to attack an American military communications system, for example, might be sitting in the basement of a publicly traded telephone company wearing a nun’s habit. Instead of a military uniform, she would be wearing the symbol of clergy—a protected group [under the law of war], and she would be sitting in a privately owned building also doubly protected by being private and vital to the well-being of society. Even assuming she is indeed a nun and not an impostor, she would nonetheless also be a combatant subject to a proportional response, such as the destruction of her own computer or the local area network.

168 Id.
sharpening it by a new body of law governing actions against non-state actors.\textsuperscript{168}

Therefore, in the case of critical national infrastructure, it is the target of the attack that should define the threat and appropriate response, not the attacker.

The United States has understood this important point, at least on the tactical military level. Under the U.S. Standing Rules of Engagement, military personnel are authorized to respond based on the target of the attack, rather than on the attacker’s identity.\textsuperscript{169} Likening these Rules of Engagement to a CNA, a nation should not be required to absorb an initial attack on its computer infrastructures before taking action. Nor should a nation have to wait until the system’s passive defenses have been fully tested in an attempt to identify the perpetrator. Regardless of the perpetrator’s identity, he has either demonstrated hostile intent or committed a hostile act by attempting to penetrate a computer system linked to critical national infrastructure. Such an intrusion must be considered an unlawful use of force under international law.

\textit{B. Characterization of the Attack}

While it is difficult to discover the identity of the attacker, identifying his intent in time to take preventive action is equally problematic and potentially more important because a victim state must identify the attacker’s intentions as hostile before it may respond with force in kind. Adding to the difficulty, CNAs can be more problematic to characterize than conventional kinetic weapons. For example, the traditional scenarios of launched weapons or marching armies provide at least some opportunity to contemplate a response. This is not the case in a CNA. There is no massing of troops on the border, and certainly no sudden increase in logistics movements. Even the precious few minutes of reaction time present in the case of a nuclear weapons launch\textsuperscript{170} are missing in a CNA.\textsuperscript{171} Once a hacker has penetrated the passive defenses of a computer system, his lethal intentions can be realized in a split second.\textsuperscript{172} A victim nation should not be precluded from taking action until after the fatal electronic signal has been sent and its harmful effects initiated.\textsuperscript{173} Rather, once

\textsuperscript{168} Schmitt, \textit{Bellum Americanum}, supra note 115, at 1073–74.

\textsuperscript{169} INSTRUCTION 3121.01A, supra note 98.


\textsuperscript{171} As mentioned previously, it is only after the passive defenses have been penetrated that the active defenses or “hack-back” would occur. Thus, there would be time prior to the penetration of the passive defenses to take intermediate steps.

\textsuperscript{172} See Souder, supra note 34.

\textsuperscript{173} It is insufficient in such a case to simply turn off the computer or sever the connection with the attacker. Not only does this allow the attacker to control the situation by forcing a continuing interruption in the ability of a nation to use its own computer systems, but it also provides no deterrent against the continuing invasion of the system. Further, as in the case of an air traffic control computer system, shutting the system down may itself create the conditions for lethal consequences. For self-defense to have any real meaning, it must not only deflect the lethal attacks of the aggressor, but must also allow for
an attacker demonstrates his intent to assail national infrastructure, the victim nation ought to attain the right to infer malicious intent and take appropriate action in self-defense. Sharp proposes 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.” Such a rule would be a step in the right direction, but would not provide comprehensive protection against nonstate actors.

As noted, the U.S. Standing Rules of Engagement have authorized military personnel a wide range of responses to an attack. More specifically, if a civilian’s actions amount to either hostile intent or a hostile act by threatening a U.S. service member, the military member is authorized and obligated to defend himself and other U.S. service members, regardless of the attacker’s identity. While this is a tactical concept of U.S. military operations, it is rooted firmly in the customary law of self-defense. The military member need not wait until the first bullet is fired, but may fire in self-defense if he has the reasonable belief that he is about to be fired upon. The hostile intent or hostile act can be inferred from the attempt to penetrate a computer system linked to critical national infrastructure. This same idea applies to CNAs as well as to traditional military attacks.

In moving national policy in this direction, President Bush should inform the international community of the United States’ intentions concerning these critical systems. The United States should publish and continually update a list of critical national infrastructure systems to give notice that these systems will be defended with an active defense. An attempt to try to hack into these systems would, in other words, be viewed as a demonstration of hostile intent to which the United States would respond proportionally in anticipatory self-

\[\text{Degradation of the aggressor’s ability to continue to commit those lethal acts. See Sirak, supra note 4, at 28; Souder, supra note 34.}\]


\[\text{[d]irectives issued by competent military authority to delineate the circumstances and limitations under which its own naval, ground, and air forces will initiate and/or continue combat engagement with other forces encountered. They are the means by which the National Command Authority (NCA) and operational commanders regulate the use of armed force in the context of applicable political and military policy and domestic and international law.}\]

\[\text{Id.}\]

\[\text{175 Sharp, supra note 57, at 149. Hostile intent is defined as “[t]he threat of imminent use of force against the United States, U.S. forces, and in certain circumstances, U.S. nationals, their property, U.S. commercial assets, and/or other designated non-US forces, foreign nationals and their property.” Id. Hostile act is defined as “[a]n attack or other use of force against the United States, U.S. forces, and, in certain circumstances, U.S. nationals, their property, U.S. commercial assets, and/or other designated non-US forces, foreign nationals and their property.” Id.}\]

\[\text{176 Id. The definitions of hostile act and hostile intent are significant because service members and their commanders have not only the authority, but also the obligation to respond to them. “A unit commander has the authority and obligation to use all necessary means available and take all appropriate actions to defend the unit, including elements and personnel, or other U.S. forces in the vicinity, against a hostile act or demonstrated hostile intent.” Id.}\]

\[\text{177 This could be accomplished through a combination of warning banners on critical national infrastructure websites, policy statements, and inclusion in government publications.}\]
defense. Furthermore, a response will occur once the passive protective measures have been penetrated. Accordingly, as a CNA is being conducted against one of these systems, the need to respond becomes "instant, overwhelming, and leaving no choice of means and no moment for deliberation."\footnote{Whiteman, Self-Defense, supra note 70, at 982; see also Schmitt, Normative Framework, supra note 33, at 931 (discussing the fact that the window of opportunity to respond in self-defense is different under different methods of attack). "Hence, the appropriate question relates more to the correct timing of the preemptive strike than to the imminence of the attack that animates it." Id.} It should be made clear that once an intruder has shown the intent and capability to pierce the passive defense measures of a critical infrastructure network, he has demonstrated sufficient hostile intent to warrant an action in self-defense, even though he may not yet have consummated his attack. In response, a nation must have the right to respond proportionally in self-defense even if the CNA does not amount to an armed attack.

\section*{C. Neutral Nations}

As argued, an active CND response is legitimate without attributing the initial attack or characterizing the attackers' intentions. Nevertheless, an active CND may be perceived as violating the rights of neutral nations in its application.\footnote{On April 14, 1986, in response to recent bombings in Europe involving U.S. soldiers, the United States conducted a bombing strike on various terrorist and military targets in Libya. President Reagan justified these actions as within the U.S.'s right of self-defense under Article 51 of the U.N. Charter. Stuart G. Baker, Note, Comparing the 1993 U.S. Airstrike on Iraq to the 1986 Bombing of Libya: The New Interpretation of Article 51, 24 GA. J. INT'L & COMP. L. 99, 106 (1994). In preparation for this strike, France denied the U.S. request to fly over its airspace in furtherance of its military operation and Spain stated after the fact that it would have denied permission had it been asked. Id. at 106 n.36. Though France and Spain may have acted out of a belief that this was not justifiable self-defense, the interaction highlights the question of the use of neutral territory in the exercise of self-defense. Even if transiting a nation's airspace might be a violation of that nation's territorial sovereignty, the DOD OGC has concluded that "use of a nation's communications networks as a conduit for an electronic attack would not be a violation of its sovereignty in the same way that would be a flight through its airspace by a military aircraft." DOD OGC, supra note 85, at 21. For an excellent discussion of neutrality in information warfare, see Walker, supra note 2.} There is, for example, a high likelihood that an attack will be routed through intermediary systems in neutral countries in an attempt to mask the perpetrator's identity:

The assailant will probably route her assault through an innocent intermediary telecommunications systems. For example, a hacker would first route her communications through various servers around the world before attempting to gain access to a [Department of Defense] computer system. In such a situation, too hasty a defender might destroy the innocent intermediate system in his effort to thwart and punish the attacker.\footnote{Shulman, supra note 137, at 948.}

Because some of these intermediary systems are likely to be in neutral nations, any active CND response targeted appropriately at the originating computer will also travel through those nations, potentially leaving a wake of destruction in its path.
The Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land applies only during times of armed conflict. However, its provisions dealing with telecommunications provide some insight into the pre-armed conflict scenario, particularly Articles 8 and 9. Article 8 removes any obligation to forbid use of telecommunications systems to belligerents, and Article 9 requires a neutral nation to apply impartially whatever actions it takes. It would therefore be a violation of the spirit and letter of the Hague Convention for a neutral country to allow an attacker to send an electronic attack over its communications lines, but disallow an active CND response over the same lines. A neutral nation is allowed to resist, by force if necessary, attempts to violate its neutrality under Article 10, but it is required to resist these attempts by both belligerents equally. Otherwise, it no longer retains its neutral status.

Additionally, under international law, “if a neutral nation is unable or unwilling to halt the use of its territory by one of the belligerents in a manner that gives it a military advantage, the other belligerent may have a right to attack its enemy in the neutral’s territory.” Certainly, if time permits, the law of neutrality would require the victim nation to contact the neutral nation and give it an opportunity to remedy the fact that the attacker is using its computer systems or servers. However, if time does not permit the victim nation to make this contact without giving the attacker the opportunity to unleash his attack—as would be the case in a CNA—the neutral nation will be unable to halt the use of its territory in an effective manner. To avoid such a situation, the victim nation should be able to respond proportionally in self-defense. These principles apply equally to the attacker’s host nation. Assuming the nation is unaware of the attacks, the victim nation is required to appeal to it to take some action, most likely based on its own domestic laws. This time-consuming requirement provides little deterrence for potential attackers. Moreover, because of the instantaneous nature of CNA, the host nation will usually be unable to intercede in a timely manner.

---

181 THE LAWS OF ARMED CONFLICTS, supra note 45, at 941.

182 Id. at 943.

Article 8. A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals.

Article 9. Every measure of restriction or prohibition taken by a neutral power in regard to the matters referred to in Article 7 and 8 must be impartially applied by it to both belligerents.

A neutral Power must see to the same obligation being observed by companies or private individuals owning telegraph or telephone cables or wireless telegraphy apparatus.

Id.

183 Id. at 943.

184 DOD OGC, supra note 85, at 6.

185 In the case of Moonlight Maze, the Russian government has been contacted and has made no efforts to stop the computer intrusions. Adams, supra note 162, at 98, 100. According to James Adams, “[L]ast year, Washington issued a demarche to the Russian government and provided Russian officials with the telephone numbers from which the attacks appeared to be originating. Moscow said the numbers were in-operative and denied any prior knowledge of the attacks.” Id. at 100.

186 Robbat, supra note 152, at para. 11.
programmed active CND in response to such an attack is not a violation of the 
host nation’s rights.

The potential effects on neutral nations, including the host nation, do not 
proscribe a victim nation’s active CND response to a CNA against critical 
national infrastructure. The victim nation is required, when feasible, to contact 
the neutral nation and the host nation from which the CNA originated. However, if that neutral nation is unaware of or has been unable to stop the 
initial CNA, or if time does not allow the victim nation to make such contact, 
the victim may reply with an active CND. This active CND must comply with 
the rules of proportionality applicable to anticipatory self-defense.

V. CONCLUSION

In assessing the current state of CNA law, the DOD OGC has concluded 
that its limitations are numerous:

In summary, the international law of self-defense would not generally 
justify acts of “active defense” across international boundaries unless 
the provocation could be attributed to an agent of the nation 
concerned, or until the sanctuary nation has been put on notice and 
given the opportunity to put a stop to such private conduct in its 
territory and has failed to do so, or the circumstances demonstrate that 
such a request would be futile.1

While most scholars agree with the DOD OGC that this is the current state of 
the law, it is an unacceptable construction. It not only fails to protect a nation’s 
national security interests, but it also strips all meaning from the doctrine of 
anticipatory self-defense. In an age of nonstate actor computer attacks, the 
current law requires that a nation must accept the first CNA, respond with only 
passive measures, and hope to control the damage until the intruder is 
identified, his intentions are discerned, and any affected neutral nations are 
contacted. If a nonstate actor is involved, the host nation must be given the 
opportunity to take domestic criminal steps against the perpetrator. All this 
must be done before the victim nation can take any active measures. In 
circumstances where a split second may mean the difference between the 
countering of an attack and the collapse of critical networks and ensuing 
damage and deaths, these unavoidable and time-consuming requirements 
would be catastrophic.

While passive CND measures are completely acceptable and a necessary 
requirement on all computer systems, they provide limited protection and are 
insufficient measures when used alone. An active component to CND must be 
available to deter and punish an intruder. The United States and other nations 
should develop robust passive and active CND programs and use them in 
response to any CNA against critical national infrastructure. As the most 
technologically advanced nation in the world, the United States should be 
proactive in advocating the legality of active CND, both to constrain pre-armed 
conflict actions by states and to deter nonstate actors. Finally, because of the 
instantaneous nature of CNA, the traditional obstacles of attribution,

187 DOD OGC, supra note 85, at 21.
characterization, and inviolability of neutrals must give way to the need for an immediate self-defense response.

This evolution of the law to allow an active defense of critical national infrastructure is vital to a complete national defense and may serve either to defeat or deter those actions posed in the scenario depicted in the beginning of this Article. Whether initiated by an enemy’s military, a terrorist organization, or an individual, CNAs will be a serious and destabilizing force unless states are given the right to protect themselves with a proportionate response in self-defense, including anticipatory self-defense, even if the attack does not constitute an armed attack.