Page 1289 - 1304 **DOI:** *https://doij.org/10.10000/IJLMH.112033*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 5

2021

Cyber Warfare: A Bane of the Modern Era

ANANYO MITRA[1]

ABSTRACT

With the passive aid of Government and private sector, the inception of a new kind of war has commenced. The United States' futile attempt to halt nuclear proliferation bore the seeds of an unknown threat. The birth of cyber warfare has taken place. The article seeks to determine what laws are present to regulate such attacks and whether the general laws of war would apply in such circumstances and how can we mitigate this problem. Society would be marred with chaos and complete disorder, countries would have to deal with political insurgencies both internally and externally and the world economy would be in shambles. This article provides an analysis of the afore-mentioned matters and attempts in discussing these issues extensively. In this article we would look into Jus Ad Bellum under which we would tend to discuss various Governing legal principles, exceptions, various self-defense measures etc.

I. INTRODUCTION

"We are detecting, with increasing frequency, the appearance of doctrine and dedicated offensive cyber warfare programs in other countries. We have identified several, based on all-source intelligence information, that are pursuing government-sponsored offensive cyber programs. Foreign nations have begun to include information warfare in their military doctrine, as well as their war college curricula, with respect to both defensive and offensive applications. They are developing strategies and tools to conduct information attacks."

- John A. Serabian, Jr., Information Operations Issue Manager, Central Intelligence Agency, before the Joint Economic Committee on Cyber Threats and the U.S. Economy, February 23, 2000.

In this present global era of substantial technological advancements, anyone who is computer savvy and is equipped with an internet connection is a potential belligerent. This article discusses a very unique kind of warfare which instead of being fought in open battlefield is being carried out within the four walls. On the hidden battlefields of history's first known cyber war, the casualties are piling up. In the U.S many banks have been hit and the telecommunications industry seriously damaged, likely in retaliation for several major attacks

[1] Author is an Assistant Professor at IFIM Law School, Bengaluru, India.

 [ISSN 2581-5369]

on Iran. Washington and Tehran are both amassing their cyber arsenal built on the base of black market digital arm bazaar, with the help of giants like Microsoft, Google and Apple.[2] With the passive aid of Government and private sector, the inception of a new kind of war has commenced. The United States' futile attempt to halt nuclear proliferation bore the seeds of an unknown threat. The birth of cyber warfare has taken place. The article seeks to determine what law are present to regulate such attacks and whether the general laws of war would apply in such circumstances and how can we mitigate this problem. The article aims also to orchestrate how the currents law be applied, adopted and amended to encounter the challenge posed by cyber attacks which has the power to ignite a war between two countries, create a state of disarray for the other nations, vitiate the principles of 'a peaceful existence of human beings'. Society would be marred with chaos and complete disorder, countries would have to deal with political insurgencies both internally and externally and the world economy would be in shambles. This article provides an analysis of the afore-mentioned matters and attempts in discussing these issues extensively.

In May 2007, the Estonian government faced the curse of cyber war- fare. An anonymous cyber attack targeted both civilian and government systems. Striking the websites of banks, ministries, newspapers, and broad- casters, the assault left Estonia without the means to tell the world it was under attack.[3] The strike was both indiscriminate and surprisingly focused: " 'Particular "ports" of particular mission-critical computers in, for example, the telephone exchanges were targeted. Packet "bombs" of hundreds of megabytes in size would be sent first to one address, then another.' "[4] This attack was more than just an inconvenience to the Estonian population: the emergency number, used to call for ambulances and the fire service, was unavailable for more than an hour. No state or terrorist group claimed responsibility after the attack, but analysts believed the complexity of the attack required the cooperation of a state and/or several large telecom firms. Given the history of the Baltic State, some naturally suspected Russian involvement. The attack on Estonia illustrates the need to confront the seriousness of cyber warfare. As leaders begin to address the problem of defending against such perilous attacks, they must not ignore the legal questions. For example, does a cyber attack constitute an "armed attack" under the United Nations Charter?[5] If analysts eventually link Russia to the attack, would the attack justify Estonia in invoking its right of self-defense under

[2] **Silent War** by Michael Joseph Gross, available at http://www.vanityfair.com/culture/2013/07/new-cyberwar-victims-american-business , accessed on 15/9/2021 at 20:47 (IST)
[3] Newly nasty, Economist, May 26, 2007,
[4] Id. (quoting Linnar Viik, who is described as "Estonia's top internet guru")
[5] See U.N. Charter art. 51

 [ISSN 2581-5369]

the Charter? Or, should the international community view the attack as a mere criminal act for the criminal justice system to look into? The recent news of individuals tied to the Chinese military hacking into the U.S. Defense Department's computer system raised very similar questions. These issues will take time to address, and yet such 'jus ad bellum' [6] issues barely scratch the surface of the legal conundrum.[7] International and military lawyers must also consider how the 'jus in bello', or international humanitarian law ("IHL"), applies to cyber warfare. For example, how would international humanitarian law apply to these at- tacks if a state of war existed between Estonia and Russia or the United States and China at the time of the attacks? Should the Geneva and Hague treaties apply to this form of warfare? While a general consensus exists that legal restrictions should apply to the use of cyber weapons in war, no apparent provision of international law explicitly bans or addresses their use.[8]

II. DEFINITION OF CYBER WARFARE

The term “cyber warfare” refers to politically motivated hacking in order to conduct espionage and sabotage. It is well established that the use of computers to manipulate markets, organizations and governments has been occurring now for decades and evidence of cyber warfare is apparent from as early as the 1970s in the form of “worm” attacks which have taken the form of extremely invasive viruses over time.[9]

It can also be defined to be " the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives".[10]

According to the Federal Bureau of Investigation (FBI), it is "the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub-national groups or clandestine agents".[11]

The U.S. National Infrastructure Protection Center[12] defined the term as, " A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence,

[6] Latin for "justice to war." It is the international legal framework that governs a state's decision to use force.
[7] See, e.g., Eric Talbot Jensen, Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self -Defense, 38 Stan. J. Int'l L. 207 (2002).
[8] Knut Dormann, Computer network attack and international humanitarian law, Inter- national Committee of the Red Cross, May 19, 2001, para. 29, http://www.icrc.org/web/eng/ siteengO.nsf/htmlall/5p2alj

[9] Available at http://www.pannone.com/media-centre/blog/cybercrime-blog/the-history-of-cyberwarfare, accessed on 15/9/2021 at 20:54 (IST)
[10] An Introduction to Cyber Crime and Cyber Law by Dr. R.K. Chaubey (2008),Publishers : Kamal Law House Kolkata, pp.145
[11] Id. pp.475
[12] National Infrastructure Protection Center, formerly a unit of the Federal Bureau of Investigation, is charged with accessing threats to critical infrastructure- particularly computer systems and providing warnings concerning

destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to particular political, social or ideological agenda".[13]

Center for Strategic and International Studies [14]defined it as, "The use of computer network to shut down critical national infrastructure (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population".[15]

III. JUS AD BELLUM

(A) Governing Legal Principles

Article 2(4) of the U.N. Charter provides that member states "*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.*"[16] This prohibition is complemented by a customary international law norm of non-intervention, which prohibits states from interfering in the internal matters of other states. The International Court of Justice ("ICJ") has held that, where the interference takes the form of a use or threat of force, the customary international law norm of non-intervention is coterminous with Article 2(4) [Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.),[17] "Acts constituting a breach of the customary principle of non-intervention, will also, if they directly or indirectly involve the use of force, constitute a breach of the principle of non-use of force in international relations."]. It is possible, however, that to the extent that cyber-attacks do not constitute a use of force, they may nevertheless violate the customary international law norm of non-intervention, as discussed below. The principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference. Expressions of *'anopinio juris'* of States regarding the existence of this principle are numerous. The Court notes that this principle, stated in its own jurisprudence, has been reflected in numerous declarations and resolutions adopted by international organizations and conferences in which the United States and Nicaragua have participated. The text thereof

threats and vulnerabilities.

[13] An Introduction to Cyber Crime and Cyber Law by Dr. R.K. Chaubey (2008),Publishers : Kamal Law House Kolkata, pp.476

[14] Center for Strategic and International Studies headquartered at Washington D.C. , serves as a strategic planning partner for the Government by conducting research and analysis and developing policy initiatives that look into future and anticipate change.

[15] An Introduction to Cyber Crime and Cyber Law by Dr. R.K. Chaubey (2008),Publishers : Kamal Law House Kolkata, pp.476

[16] http://www.un.org/documents/ga/res/37/a37r010.htm

[17] 1986 I.C.J. 14, para. 209 (June 27)

testifies to the acceptance by the United States and Nicaragua of a customary principle which has universal application. As to the content of the principle in customary law, the Court defines the constitutive elements which appear relevant in this case: a prohibited intervention must be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely (for example the choice of a political, economic, social and cultural system, and formulation of foreign policy). Intervention is wrongful when it uses, in regard to such choices, methods of coercion, particularly force, either in the direct form of military action or in the indirect form of support for subversive activities in another State.

With regard to the practice of States, the Court notes that there have been in recent years a number of instances of foreign intervention in one State for the benefit of forces opposed to the government of that State. It concludes that the practice of States does not justify the view that any general right of intervention in support of an opposition within another State exists in contemporary international law; and this is in fact not asserted either by the United States or by Nicaragua.)[18]

Nonetheless, the general consensus is that Article 2(4) prohibits only armed force. The historical background of Article 2(4) shows that it was conceived against a background of international efforts to eliminate unilateral recourse to armed force.28 Measures of economic and political coercion were not the issue. The ICJ has held that financing armed insurrection does not constitute force, indicating that other economic measures that are even less directly related to armed violence would not constitute prohibited force either. There remains some ambiguity, however, as to the extent to which Article 2(4) prohibits non-military physical force, such as flooding, forest fires, or pollution. Discussions about cyber-attacks have the potential to reignite debates over the scope of Article 2(4). Because it is much less costly to mount cyber-attacks than to launch conventional attacks, and because highly industrialized states are generally more dependent upon computer networks and are more vulnerable to cyber-attacks, cyber-attacks may prove to be a powerful weapon of the weak. This change in the cost structure of offensive capabilities may both increase the likelihood of cyber-attacks and change the political valence of different interpretations of Article 2(4)'s scope. Stronger states may begin to favor more expansive readings of Article 2(4) that prohibit coercive activities like cyber-attacks.[19]

[18] http://www.icj-cij.org/docket/index.php?sum=367&p1=3&p2=3&case=70&p3=5

[19] Walter Sharp has advocated that the United States make precisely this kind of strategic interpretive move, arguing that a broad array of coercive cyber-activities should fall within Article 2(4)'s prohibition. WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 129-33 (1999)

At the same time, there are preliminary indications that cyber-attacks as defined in this Article may violate the customary international law norm of nonintervention. First, states generally do not engage in cyber-attacks openly, but rather tend to try to hide their responsibility through technical means and by perpetrating the attacks through non-state actors with ambiguous relationships with state agencies. As Thomas Franck has observed, *"Lying about facts . . . is the tribute that scofflaw governments pay to international legal obligations they violate."* In other words, the very fact that states attempt to hide their cyber-attacks may betray a concern that such attacks may constitute unlawful uses of force. Second, when states acknowledge that they have been victims of cyber-attack, they and their allies tend to denounce and condemn the attacks.

(A) The Two Exceptions from Collective Security and Self Defence

The first exception falls under Article 39 of the U.N. Charter. Article 39 empowers the Security Council to "determine the existence of any threat to the peace, breach of the peace, or act of aggression, and [to] make recommendations, or decide what measures shall be taken . . . to maintain or restore international peace and security." The Security Council may employ "measures not involving the use of armed force" and authorize "actions by air, sea, or land forces." Collective security operations under Article 39 can be politically difficult, however, because they require authorization by the often deadlocked or slow-moving Security Council. Moreover, lawful collective security operations are easily identifiable and relatively uncontroversial. If the Security Council authorizes a use of force in response to, or in the form of, a cyber-attack, a state's lawful actions will likely be within the scope of that authorization.

The second exception to Article 2(4) is articulated in Article 51, which provides that "nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs. It is clear, however, that the critical question determining the lawfulness of self-defense is whether or not an armed attack has occurred. Many people all over the world agree that a cyber-attack may rise to the level, which may take the shape of an armed attack.

The term "armed attack" is linguistically distinct from and has been interpreted to be substantively narrower than several other related terms in the U.N. Charter. For example, there may be acts that violate Article 2(4)'s prohibition on the use or threat of force that do not rise to the level of an armed attack and do not trigger the right of self-defense under Article 51. The ICJ has indicated that cross-border incursions that are minor in their "scale and effects" may be classified as mere "frontier incidents" rather than "armed attacks." Instead, armed attacks

 [ISSN 2581-5369]

must be of sufficient gravity to constitute "most grave forms of the use of force." This does not leave states unable to respond to low-level violations of their sovereignty; even if they may not resort to defensive force, states may engage non-forceful countermeasures. Determining that "the First use of armed force by a State in contravention of the Charter shall constitute prima facie evidence of an act of aggression although the Security Council may . . . conclude that a determination that an act of aggression has been committed would not be justified in the light of other relevant circumstances, including the fact that the acts concerned or their consequences are not *of sufficient gravity*". Scholars generally agree that there is a gap between the prohibition on the use of force and the right of self-defense.[20] To the extent that cyber-attacks do not qualify as armed attacks triggering the right of self-defense, countermeasures could potentially take the form of responsive cyber-attacks (provided that they did not constitute a use of force in violation of treaty and customary international law and that the need to induce a return to compliance with international law still exists).[21] Not every cyber-attack constitutes an armed attack. In scholarly debates over the application of *jus ad bellum* to cyber-attacks, three leading views have emerged to determine when a cyber-attack constitutes an armed attack that triggers the right of armed self-defense: the instrument-based approach, the target-based approach, and the effects-based approach.[22]

One scholar has given the soubriquet "instrument-based" to the classical approach to the armed attack inquiry.[23] Under this view, a cyber-attack alone will almost never constitute an armed attack for purposes of Article 51 "because it lacks the physical characteristics traditionally associated with military coercion"—in other words; because it generally does not use traditional military weapons. This approach treats a cyber-attack as an armed attack only if it

[20] http://www.icj-cij.org/docket/index.php?sum=367&p1=3&p2=3&case=70&p3=5

[21] OFFICE OF GEN. COUNSEL, DEP'T OF DEF., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS (Nov. 1999), *reprinted in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW

[22] Once a state has been the victim of an armed attack, a further question arises as to against whom the state can respond. Where the armed attack is perpetrated by a state, this question is easily answered—self-defense may be directed against the perpetrating state. However, cyber-attacks may be perpetrated by non-state actors or by actors with unclear affiliations with state security agencies. Although some scholars argue that cyber-attacks (and conventional attacks) must be attributable to a perpetrating state in order for the victim state to take defensive action that breaches another state's territory, others—drawing on traditional jurisprudence on self-defense—argue that states possess the right to engage in self-defense directly against non-state actors if certain conditions are met. *See* Jordan J. Paust, *Self-Defense Targetings of Non-State Actors and Permissibility of U.S. Use of Drones in Pakistan*, 19 J. TRANSNAT'L L. & POL'Y (forthcoming 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1520717 ("The vast majority of writers agree that an armed attack by a non-state actor on a state, its embassies, its military, or other nationals abroad can trigger the right of self-defense addressed in Article 51 of the United Nations Charter, even if selective responsive force directed against a non-state actor occurs within a foreign country.").

[23] Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 909 (1999);

uses military weapons. For example, bombing computer servers or Internet cables could meet the requirements of an armed attack if the strike was of sufficient gravity. The text of the U.N. Charter provides some support for the instrument-based approach, since Article 41 characterizes the "partial or complete interruption of telegraphic, radio, and other means of communication" as a "measure not involving the use of armed force. The U.N. General Assembly's Definition of Aggression also implicitly supports the instrument-based view: it lists a number of acts that would constitute "aggression" under Article 39—a broader category than armed attack under Article 51—and all of them involve military weapons or force.[24] NATO has also signaled its agreement with this view; its new common approach to cyber-defense establishes that a cyber-attack will obligate member states to "consult" with one another under Article 4 of the NATO treaty, but a cyber-attack will not constitute an armed attack that obligates member states to assist one another under Article 5 of the treaty.[25] The instrument-based approach's chief advantage is simplicity of application, since uses of military weapons and force are relatively easy to identify. However, because cyber-attacks have the potential to cause catastrophic harm without employing traditional military weapons, most scholars have rejected the instrument-based approach to defining armed attacks as dangerously outdated. Recognizing the fundamental inability of the instrument-based approach to account for harms not caused by conventional means, the target-based approach classifies as an armed attack any cyber-attack that targets a sufficiently important computer system.[26] The primary aim of this approach is to determine when a cyber-attack portends imminent and sufficient harm to justify the use of anticipatory self-defense in response.[27]

While the target-based approach has the benefit of allowing for aggressive protection of critical national systems, it broadly sanctions forceful self-defense, increasing the likelihood that cyber-conflicts will escalate into more destructive conventional armed conflicts.[28]

---

[24] :- Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 ICJ 14, para. 195 (June 27) *cf.* Definition of Aggression,(article 2)

[25] NATO Agrees on Common Approach to Cyber Defence http://www.euractiv.com/en/infosociety/nato-agrees-common-approachcyber-defence/article-171377

[26] Walter Sharp, the leading proponent of this approach, argues that a cyber-attack constitutes an armed attack, and would grant the target the right to use force in self-defense, whenever it penetrates any critical national infrastructure system, regardless of whether it has yet caused any physical destruction or casualties. SHARP, *supra* note 82, at 129-30; *see also* Sean M. Condron, *Getting it Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 403, 415-16 (2007) (advocating a similar approach); Eric Talbot Jenson, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 208-09 (2002) (same).

[27] Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. at 1041 n.73.

[28] *See* Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect their Duty to Prevent*, 201 MIL. L. REV. 1, 74-75 (2009). (criticizing the target-based approach for encouraging escalation and advocating an effects-based approach).

 [ISSN 2581-5369]

Finally, the effects-based approach classifies a cyber-attack as an armed attack based on the gravity of its effects. Steering a middle course between the instrument- and target-based views, the effects-based approach is the most promising and most widely accepted approach. Different versions of the effects-based approach may measure that gravity by reference to any of a variety of factors, from the sheer severity of the harm to the length of the causal chain between the cyber-attack itself and the ultimate harm. But all versions of this approach share a common orientation towards the inquiry. The problem with the effects-based approach, however, lies in articulating *ex ante* what types of effects justify self-defense.[29] Consider, for example, an attack on an air traffic control system, an attack that disables a regional electrical power grid an attack on the New York Stock Exchange or national financial networks, or the 2007 cyber-attack on prominent Estonian websites. Which of these cyber-attacks, if any, have effects large enough to be considered armed attacks justifying the use of defensive force in response? All of these attacks may cause small- or large-scale civilian deaths and infrastructure damage, but it would be difficult for the aggressor country to predict the outcome of any individual attack. Different versions of the effects-based approach may reach different conclusions for each of these examples.

Professor Michael Schmitt, the first proponent of the effects-based approach for determining when a cyber-attack should be considered an armed attack, argues that a cyber-attack's effects should be measured by reference to six factors: (1) severity, the type and scale of the harm; (2) immediacy, how quickly the harm materializes after the attack; (3) directness, the length of the causal chain between the attack and the harm; (4) invasiveness, the degree to which the attack penetrates the victim state's territory; (5) measurability, the degree to which the harm can be quantified; and (6) presumptive legitimacy, the weight given to the fact that, in the field of cyber-activities as a whole, cyber-attacks constituting an armed attack are the exception rather than the rule.[30]

These factors are illuminating, but they call for such a wide-ranging inquiry that they may not provide sufficient guidance to decision makers.[112] In other words, different analysts applying this version of the effects-based approach might plausibly classify all or none of the examples listed above as armed attacks.[31] Daniel Silver, former General Counsel of the CIA and National

[29] This difficulty is aggravated by the reality that "the indirect effects" of cyber-attacks are often "more consequential" than the immediate ones. COMM. ON OFFENSIVE INFORMATION WARFARE, ET. AL., NAT'L RES. COUNCIL, TECHNOLOGY, POLICY LAW AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES (WILLIAM A. OWENS, ET. AL. EDS., 2009)

[30] Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L

[31] Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U.J. INT'L L. &

Security Agency, argues instead that the key criterion determining when a cyber-attack constitutes an armed attack is the severity of the harm caused. A cyber-attack justifies self-defense "only if its foreseeable consequence is to cause physical injury or property damage and even then, only if the severity of those foreseeable consequences resembles the consequences that are associated with armed coercion."[32] Of course, foreseeability is a notoriously malleable and indeterminate legal requirement, since it is extremely difficult to specify in advance exactly how long a causal chain must stretch before it is no longer appropriate to find liability—particularly in the area of cyber-attacks. This test would treat an attack on the air traffic control system causing planes to crash as an armed attack and might treat an attack disabling a regional electrical grid as an armed attack. But it would not treat attacks on websites, or even mere penetration of critical computer systems, as armed attacks. Attacks on financial systems present a hard case for this approach—the analysis depends on whether one considers scrambled financial information to be "property damage."

It is also important to note that purpose of the attack is already accounted for in the definition of cyber-attack recommended herein—that is, that the attack must have been committed for a political or national security purpose. Therefore unintended national security consequences of an attack, should the attack not have had national or security purposes at the outset, would not be considered a considered a cyber-attack or cyber-warfare under this definition.

(C) AD Bellum Necessity & Proportionality

In addition to overcoming Article 2(4)'s prohibition on the use of force, a state's use of armed force in response to a cyber-attack must also comply with the jus ad bellum principles of necessity and proportionality under customary international law. The principle of necessity requires that force must be used only as a last resort, when peaceful means, such as a diplomatic settlement, cannot achieve the state's overall aim.[33] Proportionality extends this logic, prohibiting force if the overall scope and intensity of force is excessive in relation to the state's

POL. 57, 85-86 (2001) (criticizing Schmitt's use of presumptive legitimacy as a criterion, as well as Schmitt's assumption that policymakers will be able to engage in a thorough factual inquiry when responding to cyber-attack.

Daniel B. Silver, *Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter, in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW at 89 (claiming that "examination of [Schmitt's] criteria suggests that virtually any event of [computer network attack] can be argued to fall on the armed force side of the line")

[32] Daniel B. Silver, *Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter, in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW

[33] R.Y. Jennings, The Caroline and McLeod Cases, 32 AM. J. INT'L L. 82, 89 (1938) (quoting Secretary of State Daniel Webster's letter to his British counterpart concerning the Caroline incident as follows: "It must be shown that admonition or remonstrance to the persons on board the Caroline was impracticable, or would have been unavailing . . . but that there was a necessity, present and inevitable, for attacking her . . . .").

actual or imminent danger.[34] The United States has acknowledged that these principles apply to military responses to cyber-attacks.[118] While principles of necessity and proportionality are clear, applying those principles to state responses to cyber-attacks is challenging. Evaluating whether an invocation of self-defense complies with the principles of necessity and proportionality is difficult and fact-intensive even for conventional attacks, and cyber-attacks present hard new questions. For example, cyber-attacks rising to the level of armed attacks may require decision makers to devise ways of measuring harm to computer networks and its indirect effects against more conventional kinds of harm in order to determine what would constitute a lawful response.

This Section demonstrates that applying the existing *jus ad bellum* framework in the context of cyber-attacks is challenging—and can address only a small subset of the broad range of cyber-attacks. An *ad bellum* analysis will be relevant for regulating the use of or response to only cyber-attacks addressed by Security Council resolutions and which meet the standard for an armed attack giving rise to a right of self-defense. Part III of this Article explores other international legal regimes that may help to regulate cyber-attacks that do not fall within these narrow boundaries. First, however, the following Section describes the law of war framework governing cyber-attacks occurring in the context of an ongoing armed conflict.

(E) Security Council Authorization of the Use of Force

Discussion of Security Council use of force authorizations within the context of cyber attacks can be brief. While the Council is certainly empowered to authorize U.N. Members to engage in both use of force and use of other measures against another state or states, it can do so only if it makes an Article 39 determination that the actions of a state constitute a "threat to the peace, breach of the peace, or act of aggression." Extensive experience has shown, however, that Article 39 determinations and resultant use of force recommendations are exceptionally difficult to achieve. Most such decisions are taken only after extensive and time consuming deliberations, and even then such decisions are subject to the veto of any permanent Security Council Member. Accordingly, given the nuanced and nebulous nature of cyber attacks, and the uncertainty about whether the Security Council will respond to such attacks in a timely manner, it seems valid to assume that a state will choose to deal with cyber attacks by exercising

[34] Robert D. Sloane, The Cost of Conflation: Preserving the Dualism of Jus Ad Bellum and Jus in Bello in the Contemporary Law of War, 34 YALE J. INT'L L. 47, 108-09 (2009) ("Ad bellum proportionality is . . . parasitic on ad bellum necessity. An act is ad bellum disproportionate if the same ad bellum objective sought by force clearly could have been achieved by diplomacy or another nonviolent strategy at a roughly comparable, or even moderately greater, cost.").

 [ISSN 2581-5369]

its right to self-defense.

(F) Self Defense Measures

A state's right to undertake self-defense measures is not one that was created by Article 51 of the U.N. Charter. The Charter merely reaffirmed this inherent customary international law (CIL) right of states to survive within the international community.[35] Thus, while an analysis of the self-defense concept must look to both the provisions of Article 51 and CIL,[36]there is firm international consensus on this very fundamental issue. While competing theories have always existed as to the types of state actions that actually constitute "armed attacks," a state unmistakably possesses both an inherent and Charter-derived right to engage in an "appropriate" self-defense response to such an attack. What is appropriate self-defense? A response is lawful if it complies with two bedrock principles of CIL – "necessity" and "proportionality."[37]

A state meets the requirement of necessity when it becomes evident that, under the prevailing circumstances, the state cannot achieve a reasonable settlement of a dispute through peaceful means. "Proportionality" requires that a state limit self-defense action to the amount of force required to defeat an ongoing attack or to deter a future attack.[38] Anticipatory self-defense deserves brief comment.10 A long established tenet of CIL, this self-defense corollary dates to the 1836 *Caroline* case, in which the United States and the United Kingdom agreed that a state might lawfully resort to self-defense measures when the "necessity of that self-defense is instant, overwhelming, and leaving no choice of means, and no moment for deliberation."[39] Inherent in the lawful exercise of this right, of course, is a state's requirement to demonstrate sufficiently the imminence of an anticipated attack. In the case of cyber attacks, such a requirement would invariably be difficult to meet, if not impossible.

(G) Can A Cyber Attack Constitute An Armed Attack?

Can a cyber attack – or a continuous series of cyber attacks – constitute an armed attack, thus triggering a victim state's right to respond forcefully through a legitimate exercise of self-

[35] "The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply: international custom, as evidence of a general practice accepted as law." Statute of the International Court of Justice, art. 38(1)(b). The key considerations in discerning CIL are thus general state practice and its acceptance as law. *See* INTERNATIONAL LAW: CASES AND MATERIALS 59 (Lori Fisler Damrosch et al. eds., 5th ed. 2009).
[36] YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 181 (4th ed. 2005).
[37] THOMAS WINGFIELD, THE LAW OF INFORMATION CONFLICT: NATIONAL SECURITY LAW IN CYBERSPACE 41-44 (2000).
[38] YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 181 (4th ed. 2005).
[39] *See* INTERNATIONAL LAW: CASES AND MATERIALS at 1134-1135.

defense? Answering this question is made no easier by the fact that the term "armed attack" is not specifically defined by treaty or any other form of international agreement. The international framework for analyzing whether certain state actions constitute armed attacks has evolved over time, and these are the legal principles that must be applied in assessing the nature of cyber attacks. The international consensus holds that criteria put forward by Jean Pictet in order to determine the existence of an international armed conflict under Common Article 2 of the 1949 Geneva Conventions also serve as a useful guide for assessing whether a particular use of force has risen to the level of an armed attack. Under this test, a use of force is deemed an armed attack when the force is of "sufficient scope, duration, and intensity."[40] As in the case of essentially all matters of international law, states and scholars interpret this test in different ways. Over the years, however, certain international instruments have evolved that have facilitated the application of Pictet's criteria. Principal among these has been the U.N. General Assembly's "Definition of Aggression" resolution. While this resolution offers no definitive definition of armed attack, it does provide examples of state actions that are deemed to qualify as such, and these have gained extensive international acceptance.[41] Though state pronouncements of this nature are helpful in the context of assessing conventional uses of force, they are of minimal value in determining when cyber attacks constitute armed attacks. To fill this void, three distinct analytical models have recently been put forward to facilitate the application of Pictet's use of force criteria – scope, duration, and intensity – to unconventional uses of force, including cyber attacks.

The first of these is an "instrument-based approach." Using this model, an assessment would be made as to whether the damage caused by a cyber attack could previously have been achieved only by a kinetic attack. For example, using this model, a cyber attack conducted for the purpose of shutting down a power grid would be deemed an armed attack. Why? Because prior to the development of cyber capabilities, the destruction of a power grid would typically have required bombing a power station or using some other form of kinetic force to achieve such result.[42]

The second analytical model is an "effects-based approach," which is often referred to as a consequence-based model. Using this approach, no attempt would be made to assess whether

[40] WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE (1999); Sean Condron, *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 404 (2007)
[41] Definition of Aggression, G.A. Res. 3314, U.N. GAOR, 29th Sess., U.N. Doc. A/RES/3314 (Dec. 14, 1974);
[42] Yoram Dinstein, *Computer Network Attacks and Self-Defense*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 99 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002),at 103-105

the damage resulting from a cyber attack could previously have been achieved only through a kinetic use of force. Here the consideration would be the overall effect of the cyber attack on the victim state. For example, using this approach, a cyber manipulation of information across a state's banking and financial institutions significantly disrupting commerce within that state would be viewed as an armed attack. That is, while such an action would bear no resemblance to a kinetic attack, the overall damage that this manipulation of information would cause to the victim state's economic wellbeing would warrant it being equated with an armed attack.[43]

The third model is one of "strict liability" that would automatically deem any cyber attack against critical national infrastructure (CNI)18 to be an armed attack, based on the severe consequences that could result from any attack on such infrastructure systems. While the merits of each of these analytical models have been extensively debated, their primary importance resides in the fact that the proponents of all three approaches agree on the singularly important conclusion that cyber attacks can constitute armed attacks.

IV. CONCLUSION

In assessing the applicability of the LOW to cyber threats, consideration must first be given to the relevant conflict management (*jus ad bellum*) principles currently determining the legitimacy of a state's use of force. A brief review of these norms has indicated that a state may lawfully resort to force when acting in self-defense against an armed attack, provided it conforms to the customary international law concepts of necessity and proportionality. In examining three analytical models developed to facilitate a determination as to whether a particular use of force has risen to the level of an armed attack, it is possible to conclude that certain cyber attacks can be deemed armed attacks. Essential to a victim state's ability to use force – in this case, active defenses against a cyber attack – is that state's ability to assign responsibility for such an attack to another state. Traditionally, this requirement could be met only by directly and conclusively attributing the attack to another state actor. Given the anonymity of cyber technology, this doctrine as traditionally applied would constitute an exceptionally difficult standard. However, there have been continuing efforts to develop viable alternatives to this "conclusive attribution" principle, all of which rely on the concept of imputed responsibility. These efforts and the events of the past twenty years have now arguably produced an imputed state responsibility standard of "indirect responsibility," which reaches a state's failure to prevent non-state actors from engaging in cyber attacks from within its

[43] THOMAS WINGFIELD, THE LAW OF INFORMATION CONFLICT: NATIONAL SECURITY LAW IN CYBERSPACE 41-44 (2000). at 117-130

 [ISSN 2581-5369]

boundaries. The notion of imputed state responsibility for cyber attacks is centered on that state's violation of what is now viewed as an established duty to prevent its territory from being used as a launching pad for attacks.

Consistent with this approach, a state is said to have breached this duty when it consistently fails to undertake specifically identified measures designed to prevent these attacks. Such measures would include passage of legislation criminalizing cyber attacks and cooperation in the investigation and prosecution of those who engage in such attacks. In essence, then, when a state exhibits either an unwillingness or inability to prevent the use of its territory by non-state actors for the purpose of launching cyber attacks, it becomes a sanctuary state. As such, it becomes vulnerable to a legitimate use of force by the victim state. The responsibility for making the key determinations associated with the use of force – the deployment of active defenses – against cyber attacks emanating from a sanctuary state is as yet unassigned. Some have urged that the need for a rapid response to such attacks dictates that these decisions be made by individual system administrators, drawing upon previously established rules of engagement. Given the potential ramifications of the use of active defenses, this would not appear to be a prudent approach. There is a need to consider all of the particulars surrounding a cyber event carefully, including those bearing on any use of force compliance with the LOW. This would dictate that the requisite decisions involved ultimately be made by those fully attuned to the political and legal risks.

Finally, while the use of active defenses rather than kinetic weaponry in responding to a cyber attack would appear to offer a greater opportunity for compliance with the basic principles of the LOW, the use of active defenses in the anonymous cyber domain will be problematic. Identifying the source of a cyber attack, particularly one routed through a series of innocent systems, and accurately mapping its course, is difficult and often time consuming. The misidentification of the attack source – or a "hack back" through innocent systems – may well result in significant violations of the LOW precepts of military necessity, discrimination, and proportionality. Given these realities, a decision to employ active defenses is, again, one that should be made only after careful consideration of the inherent legal and political risks. The goal of this article has been to provide a brief and succinct assessment of the manner in which both conflict management principles and the LOW might be applied to cyber threats. These principles should, and do, control the use of any kinetic and active defense measures that might be taken against cyber attacks. Lest there be any doubt, this law is real and must be applied. The ongoing challenge, then – given the inherent difficulties involved – is that of developing workable procedures that will enable national leaderships to respond effectively to cyber

 [ISSN 2581-5369]

attacks within the bounds of this law.

*****

 [ISSN 2581-5369]