Cyber Threats and the Law of War

David E. Graham*

INTRODUCTION

When I was invited to participate in a forum dealing with "National Security Threats in Cyberspace," sponsored by the American Bar Association Standing Committee on Law and National Security and the National Strategy Forum, my assigned role was to provide a "succinct and brief" explanation of how the existing Law of War (LOW) might be applied to cyber threats. The *Journal of National Security Law & Policy* later requested that I reduce my comments to writing. No doubt this generous request was made due to the brevity of my analysis, rather than to my intellectual prowess. Others have dealt with this subject in a far more detailed and sophisticated fashion.[1] Nevertheless, for non-lawyer decisionmakers who must constantly struggle with this matter, brevity and succinctness appear to have a tangible appeal. It is in this vein that I offer the following thoughts.

I. IT'S NOT JUST THE LAW OF WAR: ENTER *JUS AD BELLUM*

In attempting to abide by the constraint of simplicity in dealing with this subject, I find that it is unfortunate, but nevertheless true, that the question of how to apply the current LOW to cyber warfare can be addressed only after it is first determined that a state might legally use "force" in responding to what it perceives to be "cyber attacks." And, in turn, this determination must be made in the context of *jus ad bellum*, those established "conflict management" norms and procedures that dictate when a state may – and may not – legitimately use force as an instrument of dispute resolution.[2]

---

* U.S. Army Colonel (Retired); Executive Director, The Judge Advocate General's Legal Center and School, U.S. Army. The author has prepared this article in his personal capacity and does not purport to present the views of the Department of Defense, the Department of the Army, or the Army's Judge Advocate General's Legal Center and School.

1. Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Which Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1 (2009), provides an excellent introduction of this subject. *See also* 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); 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); Eric 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).

2. *See* John Norton Moore, *Development of the International Law of Conflict*

While *jus ad bellum* is not exclusively the domain of the U.N. Charter, the following Charter provisions are mostly relevant to the topic at hand:

- Article 2(4): 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.

- Article 39: The 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.

- Article 51: Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.[3]

While international lawyers have endlessly debated the "real" meaning of Article 2(4), for our purposes, let us take its wording at face value. This provision prohibits a state from either threatening or using "force" against another state in the international community. And as reflected in Articles 39 and 51, only two exceptions exist to this absolute use of force prohibition: actions authorized by the Security Council and acts of self-defense.

A. Security Council Authorizations 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,[4] it can do so only if it makes an Article 39 determination that the actions of a state constitute a

---

Management, *in* NATIONAL SECURITY LAW 29, 29 (John Norton Moore & Robert F. Turner eds., 2d ed. 2005); John Norton Moore, *The Use of Force in International Relations: Norms Concerning the Initiation of Coercion*, *in* NATIONAL SECURITY LAW, *supra*, at 69, 69-70.

3. U.N. Charter arts. 2(4), 39, 51.

4. *Id.* arts. 41, 42.

"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 arrived at only after extensive and time consuming deliberations, and even then such decisions are subject to the veto of any permanent Security Council Member.[5] 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 its right to self-defense.

B. 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.[6] Thus, while an analysis of the self-defense concept must look to both the provisions of Article 51 and CIL,[7] 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."[8] 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 actions to the amount of force required to defeat an ongoing attack or to deter a future attack.[9] Compliance with this latter principle is obviously dependent on the particular factual situation.

Anticipatory self-defense deserves brief comment.[10] A long established tenet of CIL, this self-defense corollary dates to the 1836 *Caroline* case, in

---

5. *Id.* art. 27.

6. "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).

7. YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 181 (4th ed. 2005).

8. THOMAS WINGFIELD, THE LAW OF INFORMATION CONFLICT: NATIONAL SECURITY LAW IN CYBERSPACE 41-44 (2000).

9. DINSTEIN, *supra* note 7, at 237.

10. MICHAEL WALZER, JUST AND UNJUST WARS 74 (1977).

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."[11] 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.

C. 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-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. This is perhaps surprising. Nevertheless, 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[12] 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."[13]

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.[14]

Though state pronouncements of this nature are helpful in the context of assessing conventional uses of force, they are of minimal value in

---

11. INTERNATIONAL LAW, *supra* note 6, at 1134-1135.

12. Article 2 in each of the four 1949 Geneva Conventions is the same, thus the use of the term "common." Article 2 states that: "[T]he present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them." *See, e.g.*, Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135.

13. *See* SHARP, *supra* note 1, at 60-61. Pictet conceived of this test to aid in the clarification of when an international armed conflict exists under Common Article 2.

14. Definition of Aggression, G.A. Res. 3314, U.N. GAOR, 29th Sess., U.N. Doc. A/RES/3314 (Dec. 14, 1974); *see* WINGFIELD, *supra* note 8, at 111.

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.[15]

The second analytical model is an "effects-based approach," often referred to as a consequence-based model. Using this approach, no attempt would be made to assess whether 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.[16] This would appear to be the analytical model adopted by the United States.[17]

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.[19]

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

---

15. *See* Dinstein, *supra* note 1, at 103-105.

16. *See* WINGFIELD, *supra* note 8, at 117-130.

17. *See* OFFICE OF GENERAL COUNSEL, DEPARTMENT OF DEFENSE, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS (May 1999), *reprinted in* WINGFIELD, *supra* note 8, at 431, 453-454.

18. "'Critical infrastructure' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Critical Infrastructure Protection Act of 2001, 42 U.S.C.S. §5195c(e) (2006).

19. *See* SHARP, *supra* note 1, at 129-131; *see also* Condron, *supra* note 1, at 415-422; Jensen, *supra* note 1, at 228-231.

conclusion that cyber attacks can constitute armed attacks.[20] With this in mind, let us now turn to the second significant issue associated with a state's ability to use force in response to a cyber attack as a legitimate exercise of the right of self-defense: the need to establish another state's responsibility for the cyber attack.

D. State Responsibility for Cyber Attacks

A state's ability to hold another state responsible for a cyber attack treated as an armed attack is an essential aspect of a victim state's right to employ "active defenses" (the use of force) in a legitimate exercise of self-defense against the responsible state.[21] Active defenses consist of electronic countermeasures that attack an aggressive computer system, immobilizing that system and thus halting the cyber attack. Given the resulting damage that would occur to the system counterattacked and, potentially, to other "innocent" systems through which the original attack might have been routed, traditional international law would dictate that a victim state might engage in a self-defense measure of this nature only if it could attribute the original cyber attack directly and conclusively to another state or agents under that state's direct control.[22]

Given the anonymity of the technology involved, attribution of a cyber attack to a specific state may be very difficult. While a victim state might ultimately succeed in tracing a cyber attack to a specific server in another state, this can be an exceptionally time consuming process, and, even then, it may be impossible to definitively identify the entity or individual directing the attack.[23] For example, the "attacker" might well have hijacked innocent systems and used these as "zombies" in conducting attacks.[24]

For these reasons, states acting on the perceived legal requirement that they must conclusively attribute a cyber attack to another state or its agents historically have chosen to respond to cross-border cyber attacks as they would to criminal matters, employing only "passive" (computer security) measures to and urging the states from which the attacks originated to investigate and prosecute those responsible. There is ample evidence, however, that even the most sophisticated computer security measures cannot completely protect a state's critical systems.[25] Even more telling,

---

20. *See* WINGFIELD, *supra* note 8, at 117-130; Dinstein, *supra* note 1, at 103-105; Condron, *supra* note 1, at 415-422; Jensen, *supra* note 1, at 228-231.

21. Michael Schmitt, *Preemptive Strategies in International Law*, 24 MICH. J. INT'L L. 540-543 (2003).

22. *See* Condron, *supra* note 1, at 415; Dinstein, *supra* note 1, at 111.

23. *See* Jensen, *supra* note 1, at 232-235 (discussing the difficulty of attributing cyber attacks across international borders).

24. *See* RICK LEHTINEN ET AL., COMPUTER SECURITY BASICS 81 (2d ed. 2006).

25. *See* ANDREW COLARIK, CYBER TERRORISM: POLITICAL AND ECONOMIC IMPLICATIONS 163 (2006).

several global players have consistently demonstrated a lack of desire to deal with cyber attacks through effective law enforcement. Indeed, just the reverse has been true.[26] The smoke screen of a state attributing cyber attacks exclusively to private individuals within a state may often serve as a convenient cover for states that might be either directing or knowingly tolerating such attacks.

Given the difficulties raised by the traditional requirement to attribute cyber attacks conclusively and directly to a state – and the increasing vulnerability to continuous attacks to which this concept exposes victim states – there is now a growing effort to formulate acceptable alternatives to the notion of "conclusive attribution."[27] While all these approaches have merit, the focus here will be on the suggestion that state responsibility for cyber attacks may be based on "imputed" responsibility.[28]

In assessing this concept, it is important to note that the idea of imputed responsibility would apply not only to cyber attacks conducted by a state's own citizens, but to all non-state actors who launch such attacks from within a state's territory. Indeed, it is now generally accepted that non-state actors, such as terrorists, have committed armed attacks against states.[29] Certain cyber attacks can rise to the level of armed attacks. Given these facts and the reality that essentially all cyber attacks are now traced to non-state actors, attention will be centered on the imputed responsibility of states for the actions.

Two key questions are associated with the concept of imputed responsibility: What is a state's duty to prevent cyber attacks? What constitutes a state's violation of this duty?[30]

E. The Duty To Prevent Cyber Attacks

Imputed state responsibility for cyber attacks is premised on the existence of an affirmative duty of states to prevent their territories from being used as launching pads for such attacks. This duty, in turn, is said to consist of the following state obligations:

- To enact stringent criminal laws against the commission of international cyber attacks from within national boundaries.

---

26. *See* Condron, *supra* note 1, at 414.

27. *See* Jensen, *supra* note 1, at 236-237; Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT'L L. & POL. 57, 103-104 (2001); Richard Garnett & Paul Clarke, *Cyberterrorism: A New Challenge for International Law*, *in* ENFORCING INTERNATIONAL LAW NORMS AGAINST TERRORISM 479 (Andrea Bianchi ed., 2004).

28. *See* Sklerov, *supra* note 1, at 38-39.

29. *See* DINSTEIN, *supra* note 7, at 187, 204.

30. *See* Sklerov, *supra* note 1, at 62-72.

- To conduct meaningful, detailed investigations into cyber attacks.
- To prosecute those who have engaged in these attacks.
- To cooperate with the victim states' own investigations and prosecutions of those responsible for the attacks.[31]

While it can be argued that these state obligations are derived from all sources of international law, several sources appear to be particularly relevant. The European Convention on Cybercrime – the most significant international agreement that speaks to this issue, ratified by states that are the largest Internet users in the world – both criminalizes cyber attacks and confirms the duty of states to prevent their territories from being used by non-state actors to conduct these attacks against other states.[32]

In terms of state practice, a growing number of U.N. declarations have dealt specifically with cyber attacks. The U.N. General Assembly has called upon states to criminalize such attacks[33] and to prevent their territories from being used as safe havens from which to launch attacks.[34] The General Assembly has also called upon member states to cooperate in the investigation and prosecution of international cyber attacks.[35] Finally, some states, including the United States, and the General Assembly have specifically identified cyber attacks as a threat to international peace and security.[36]

F. Violation of the Duty To Prevent Cyber Attacks: Becoming a Sanctuary State

The assessment of whether a state has violated its duty to prevent cyber attack by providing a sanctuary for non-state actors engaging in such attacks across international borders depends on certain facts. When making such an assessment, a victim state must at a minimum examine a sanctuary state's criminal law dealing with cyber attacks, its enforcement of the law, and its demonstrated record of cooperating with victim states' own investigations and prosecutions of cyber offenders who have acted across borders.[37] Thus, a sanctuary state's benign indifference to cyber attacks continuously launched from within its borders, its failure to investigate and

---

31. *Id.* at 62.

32. *See* Convention on Cybercrime, Council of Europe, Nov. 23, 2001, 41 I.L.M. 282, 2296 U.N.T.S. 167 (ratified by the United States in 2006).

33. G.A. Res. 45/121, ¶3, U.N. Doc. A/RES/45/121 (Dec. 14, 1990).

34. G.A. Res. 55/63, ¶1, U.N. Doc. A/RES/55/63 (Jan. 22, 2001).

35. G.A. Res. 45/121, *supra* note 33, ¶3.

36. *See* THE NATIONAL STRATEGY TO SECURE CYBERSPACE 49-52 (2003), *available at* http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf (noting the threat that cyber attacks pose to international peace and security).

37. *See* Sklerov, *supra* note 1, at 62.

prosecute those responsible, and its refusal to cooperate with the efforts of victim states to deter such attacks leave it vulnerable to charges of imputed responsibility for these actions.

G. Imputing Responsibility for Cyber Attacks by Non-State Actors

Historically, states were not held responsible for the actions of non-state actors. Responsibility resulted only from those actions taken by the state itself, and from the actions of state "agents," individuals over whom the state exercised direct authority.[38] The standard for assessing state responsibility was referred to as the "effective control test," established by the International Court of Justice (ICJ) in *Nicaragua v. the United States*. In this instance, though the United States had financed, organized, trained, and equipped Contra rebels fighting against the Nicaraguan government, the ICJ failed to hold the United States responsible for the Contras' actions. Instead it was the view of the Court that while the United States had indeed provided decisive support to the Contras, a state could not be held legally responsible for the actions of non-state actors unless that state "had effective control of the military or paramilitary operations in the course of which the alleged violations were committed."[39]

Events over the past twenty years have resulted in substantial modifications of the effective control standard for assigning state responsibility for the actions of non-state actors. In 1999, the International Criminal Tribunal for the former Yugoslavia (ICTY) opined that a state could be held responsible for the actions of a militarized group when that state had coordinated or assisted in the general planning of the group's military activity. In essence, this marked a shift from the effective control test to one of a state's "overall control" of non-state actors for the purpose of imputing state responsibility for the actions of non-state groups using a state's territory as a base of operations.[40]

Since 1999, a further shift has occurred in the standard to be used in determining imputed state responsibility for the actions of non-state actors. This is evidenced by the International Law Commission's adoption of the Draft Articles on the Responsibility of States for Internationally Wrongful Acts – and the U.N. General Assembly's recognition of this document.[41]

---

38. *See* Vincent-Joël Proulx, *Babysitting Terrorists: Should States Be Strictly Liable for Failing To Prevent Transborder Attacks?*, 23 BERKELEY J. INT'L L. 616, 619-620 (2005).

39. *Id.* at 620-621 (quoting the Nicaragua case, Military and Paramilitary Activities In and Against Nicaragua (Nicar. v. U.S.), 1984 I.C.J. Rep. 392).

40. *Id.* (referring to the Tadić case, Prosecutor v. Tadić, Case No. IT-94-1-A, I.C.T.Y. App. Ch., at 49 (July 15, 1999)).

41. *See* International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts* (2001), *available at* http://www.ilsa.org/jessup/jessup06/basicmats2/DASR.pdf.

These Draft Articles reflect an emerging consensus that any breach of a state's international obligations to other states, whether in the form of treaty or customary law, will result in international responsibility. This breach can be the result of a specific state action – or, importantly, a failure to act.[42]

This evolving consensus regarding the establishment of a new standard for imputed state responsibility solidified following the September 11 terrorist attacks on the United States. The events of September 11, 2001, and the reaction of the international community to them served to effect a fundamental shift from the state responsibility standard of effective control to one of "indirect responsibility." While the al Qaeda terrorists who perpetrated what was deemed an armed attack on the United States were based in Afghanistan, there was no indication that the Taliban government had exercised effective – or even overall – control over al Qaeda.[43] Nevertheless, the international community concluded that because the Taliban had provided a sanctuary to al Qaeda – and had continued to do so even after being warned to desist – al Qaeda's September 11 actions were imputable to the Taliban government.[44]

In sum, following the September 11 attacks, state responsibility for the actions of non-state actors can be said to result from a state's failure to meet its international obligation to prevent its territory from being used by such actors as a base from which to launch attacks on other states.[45] In the case of cyber attacks, a determination of such imputed responsibility takes us back to an assessment of the questions suggested previously: Has there been a continuous pattern of cyber attacks originating from the state in issue? Has this state criminalized such actions? Has this state actively investigated and prosecuted those individuals responsible for such attacks? If the state lacks the capacity to investigate and prosecute those who have committed cyber attacks, has it sought assistance to enable it to do so? And, finally, has this state actively cooperated in the victim state's investigation and prosecution of those responsible for such attacks? Answers to these questions will greatly facilitate a determination as to whether a state has, in fact, demonstrated through its failure to prevent cyber attacks that it has become a sanctuary state with imputed responsibility for the damage resulting from these attacks.

H. Who Makes the Critical Decisions?

Critical judgments will need to be made prior to any application of basic LOW principles to a use of force in response to a cyber attack or series of attacks. Let there be no doubt that in a real world environment,

---

42. Proulx, *supra* note 38, at 622-623.

43. *Id.* at 635-636.

44. *Id.* at 637-641.

45. *See* TAL BECKER, TERRORISM AND THE STATE: RETHINKING THE RULES OF STATE RESPONSIBILITY 3 (2006).

answering the following questions will be difficult – subject to both second guessing and criticism:

- Does a single cyber attack – or a series of such attacks made over a period of time – constitute an armed attack?
- Has the state from which these attacks were launched demonstrated that it has become a sanctuary state?
- Who will make these decisions?

Some have advocated that given the perceived need for a timely – if not immediate – response to a damaging cyber attack, system administrators must ultimately determine both whether an armed attack has occurred and, if so, whether the state from which the attack was launched may, in fact, be identified as a sanctuary state.[46] Having made these determinations, a system administrator would then also have to make critical decisions regarding the rapid employment of active defense measures that would meet the use of force requirements of the LOW. Is this a workable approach?

This decision tree issue is perhaps the most difficult when attempting to formulate a workable policy for employing active defense measures against cyber attacks. The legal and policy ramifications associated with the use of such measures are significant. Consider the difficulties confronting those who must make the decisions in question. While automated and administrator-operated trace programs can undoubtedly facilitate the tracking of an attack to its point of origin, substantial technological obstacles stand in the way of an administrator's ability to identify the specific source of an attack rapidly and assess both the damage that has occurred and that which is likely to result.[47] In addition to these technical difficulties, there is the somewhat abstract, but consistently debated, matter of whether the individual who actually initiates active defense measures must wear a uniform. That is, given the principle of distinction, must the person who physically presses "send" in an active defense scenario be viewed as a lawful "combatant" under the Law of War?

Given these realities, a rapid response to a cyber attack, even one that can legitimately be deemed an armed attack, is unlikely to be a viable option. A state may craft readily available rules similar to rules of engagement for use by system administrators in making the determinations in issue. However, decisions inherent in the use of active defense measures

---

46. *See* David Wheeler & Gregory Larsen, *Techniques for Cyber Attack Attribution*, INST. DEF. ANALYSIS, Oct. 2003, at 23-24, *available at* http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859&Location=U2&doc=GetTRDoc.pdf.

47. *See generally id.* at 9-42, 51-52 (discussing technical issues related to tracing cyber attacks to their points of origin).

in response to a cyber attack are so fraught with policy considerations and risks of conflict escalation that it is most doubtful that individual system administrators will be authorized to make these determinations. Given the current technological limitations on attack identification and assessment, these matters, almost invariably, will be dealt with at a much higher level of command, employing an intricate deliberative process. Such a process would include the following steps:

- Sanctuary states will have been identified.
- Prior attacks will have been documented.
- Those attacks giving rise to a potential active defense response will have been distinguished.
- LOW issues related to the use of active defense measures will have been assessed.

It is to the consideration of these LOW matters that we may now finally turn.

II. *JUS IN BELLO* AND CYBER ATTACKS

An analysis of the applicability of the LOW to cyber attacks must center on four universally accepted LOW principles:

1. "Military Necessity" authorizes the use of force required to accomplish the mission. It does not authorize acts otherwise prohibited by the LOW. This principle must be applied in conjunction with other LOW principles, as well as with other more specific legal constraints set forth in LOW international agreements to which the United States is a party.
2. "Distinction" or "Discrimination" requires that combatants be distinguished from noncombatants and that military objectives be distinguished from protected property or protected places. Parties to a conflict are to direct their operations only against combatants and military objectives.
3. "Proportionality" mandates that the anticipated loss of life and damage to property incidental to attacks must not be excessive in relation to the concrete and direct military advantage expected to be gained.
4. "Unnecessary Suffering" ("Humanity") dictates that a military force must minimize unnecessary suffering. It is forbidden to employ arms, projectiles or material calculated to cause unnecessary suffering. This principle constrains the choice of

> weapons and ammunition, as well as regulating the methods through which such weapons and ammunition are employed.[48]

The applicability of these basic LOW principles to cyber attacks will be assessed here exclusively in terms of the use of active defense measures – that is, electronic countermeasures designed to strike an attacking computer system, shut it down, and halt an attack. This approach results from the fact that while a state responding to a cyber attack in a legitimate exercise of its right of self-defense might legally choose to employ kinetic weapons to terminate such an attack, the discussion that follows will demonstrate that such a choice would render compliance with the LOW much more problematic.

In terms of military necessity, active defense measures represent, in the great majority of cases, the degree of force necessary to accomplish the military mission – that is, to shut down the attacking computer system. The use of kinetic weaponry to attack the system in issue would generally not only be less effective, it would constitute a disproportionate use of force. This action might well be viewed as retaliatory in nature, one designed to "punish" the sanctuary state, and as such a violation of the LOW.

While some would disagree,[49] I contend that active defense measures when assessed in the context of the principles of proportionality, distinction, and unnecessary suffering are a better choice than kinetic force from the standpoint of LOW compliance. The traceback capabilities of active defenses will ensure that these measures target only the source of the cyber attack. In turn, this would accomplish the following: greatly reduce collateral damage relative to that which would result from the use of kinetic weaponry, thus helping to achieve proportionality; distinguish the attacking system (the military objective) from protected places, property, and civilians; and minimize the unnecessary suffering that would be the probable result of a kinetic use of force. Having said this, however, it is apparent that the use of active defenses to defeat cyber attacks will also create substantial difficulties with regard to LOW compliance.

While their use would arguably be more compliant with the LOW than the use of kinetic means to counter a cyber attack, the employment of active defenses will also run a very real risk of triggering LOW violations. A "surgical" strike against a computer system ostensibly at the core of a cyber attack may not be possible to achieve due to technical limitations. It is exceptionally difficult to trace an attack routed through intermediary systems. When such an attack occurs, a trace program not only requires

---

48. *See* INTERNATIONAL AND OPERATIONAL LAW DEPT., JUDGE ADVOCATE GENERAL'S LEGAL CENTER AND SCHOOL, OPERATIONAL LAW HANDBOOK 12-14 (2008).

49. Ruth Wedgwood, *Proportionality, Cyberwar, and the Law of War*, *in* 76 COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 219, 227-230 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002).

time to carry out its function, but it becomes more difficult to pinpoint the specific source of the attack once the attacker terminates the electronic connection. This may well cause a failure to identify the attacking system or an incorrect identification of an intermediary system as the source of the attack, with potentially significant LOW implications.[50]

Additionally, even when the source of an attack can be identified, a system administrator must then "map" the attacking system – assessing its functions and attempting to make an informed decision of the likely consequences (resulting damage) that will occur if actions are taken to shut the system down. This, too, will take time, and there is substantial risk in employing active defenses against a system that has not been fully mapped. To do so may well lead to accidental targeting of innocent systems, resulting in unintended and excessive collateral damage.[51]

A state might contend that in turning to the use of active defenses in a particular situation it had taken all feasible efforts to identify an attacking system and to evaluate the probable collateral damage that would result from its actions.[52] Nevertheless, the extent of the damage that actually occurs when a state employs such defenses, particularly in relation to innocent systems located in third states, may likely be viewed as violations of both the principles of distinction and proportionality and thus violations of the LOW. For example, such would be the case if the use of active defenses against an attacking system either routed through – or intricately tied to – CNI systems of either the host or third states were to result in unanticipated and substantial damage to these systems.

In sum, while from the standpoint of LOW compliance, the use of active defenses to take down an attacking computer system would arguably appear to be more appropriate than the employment of kinetic means, active defenses are not panaceas. The utilization of these measures gives rise to significant concerns. The currently available technology upon which active defenses depend leaves ample room for error and, consequently, unintended consequences. Their use will require very careful consideration by policy makers, from both legal and strategic perspectives.

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

---

50. *Id.*; *see also* Wheeler & Larsen, *supra* note 46, at 23-55 (discussing methods to trace cyber attacks to their source); Barkham, *supra* note 27, at 82-83; Eric Jensen, *Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations?*, 18 AM. U. INT'L L. REV. 1145, 1178-1179 (2003).

51. Jensen, *supra* note 50, at 1178-1179.

52. *Id.* at 1186.

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 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 attacks within the bounds of this law.