Volume 56 | Issue 3 Article 10

2011

Cyber Operations and the Jud Ad Bellum Revisited

Michael N. Schmitt

2011]

CYBER OPERATIONS AND THE *JUS AD BELLUM* REVISITED

MICHAEL N. SCHMITT*

OVER a decade ago, Professor John Murphy and I presented papers at a U.S. Naval War College conference on Computer Network Attack and International Law.[1] At the time, I was an Air Force officer assigned to the College and he an eminent scholar at Villanova University School of Law. Professor Murphy generously and graciously took me under his wing and has been a cherished mentor ever since. It was a particular pleasure to serve as the Naval War College's 2007-2008 Charles H. Stockton Professor, a post which Professor Murphy held with great distinction in 1980-1981. Over the years, it has also been my good fortune to become close friends with him. Therefore, it is a tremendous honor for me to contribute to this effort to mark Professor Murphy's long and distinguished service to our nation, the international law community, and Villanova University. I do so by revisiting the topic that began our friendship: cyber operations.

I. INTRODUCTION

In April and May 2007, Estonia was victimized by massive computer network attacks.[2] The incident began with rioting incited by ethnic Russian cyber agitators in response to the government's decision to move a Soviet war memorial from the center of Tallinn to a military cemetery on the outskirts of the capital. Subsequent actions included direct cyber attacks against Estonian targets, including government and commercial Internet infrastructure and information systems such as the those of the President, Prime Minister, Parliament, State Audit Office, ministries, political parties, banks, news agencies, and Internet service providers. They involved denial of service (DoS), distributed denial of service (DDoS), defacement, and destruction.

* Chairman, International Law Department, US Naval War College. The views expressed in this Article are those of the author in his personal capacity and do not necessarily represent those of the US Navy or any other US government entity. This Article benefitted from the generous support of the National Research Council of the National Academies. It is based in part on Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts, in* DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 151 (2010), portions of which are reproduced with permission.

1. The proceedings of the 1999 conference were published as 76 INTERNATIONAL LAW STUDIES: COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW (Michael N. Schmitt & Brian O'Donnell eds., 2002).

2. For an excellent discussion of the attacks, see ENEKEN TIKK ET AL., INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 14-33 (2010).

Because Estonia had invested heavily in networking following independence, the attacks proved devastating. By 2007, the country relied on information services for everything from banking and filing tax returns to paying for parking and public transportation. Internet services covered all of Estonia, with half the population enjoying access from their homes.

Most of the attacks emanated from outside the country, principally Russia. Their origin was also traced to at least 177 other countries.[3] Initially, they came from private IP addresses, although experts tracked a number to Russian government institutions. It remains uncertain whether the latter were launched with the government's knowledge. As the cyber attacks unfolded, they became increasingly sophisticated, evidencing considerable organization and command and control. While various pro-Russian activist groups apparently executed some of the second-wave operations, there is no firm evidence that the Russian government either conducted or orchestrated them.

The impact of the cyber assault proved dramatic; government activities such as the provision of state benefits and the collection of taxes ground to a halt, private and public communications were disrupted, and confidence in the economy plummeted. But what was the legal character of the incident?

In the aftermath of the Second World War, the international community crafted a new normative scheme in the form of the United Nations Charter, which includes both a prohibition on the use of force in international relations and a system for enforcing the proscription. Today, the Charter, together with related customary international law norms,[4] governs how and when force may be employed by States.

This Article explores the contemporary international law governing cyber operations. In particular, it asks three questions relevant to the Charter scheme governing the use of force in international relations:

1) When does a cyber operation constitute a wrongful "use of force" in violation of Article 2(4) of the United Nations Charter and customary international law?;
2) When does a cyber operation amount to a "threat to the peace, breach of the peace, or act of aggression," such that the Security Council may authorize a response thereto?; and
3) When does a cyber operation constitute an "armed attack," such that the victim-state may defend itself, even kinetically, pursuant to the right of self-defense set forth in Article 51 of the UN Charter and customary international law?

3. *See* Charles Clover, *Kremlin-Backed Group Behind Estonia Cyber Blitz*, FIN. TIMES, Mar. 11, 2009, http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html#axzz1DtPlzO27.

4. For a further discussion of customary international law, see *infra* note 13 and accompanying text.

The attacks against Estonia, similar ones against Georgia during its armed conflict with Russia in 2008,[5] and the thousands of others directed against government, corporate, and private systems worldwide on a daily basis aptly demonstrate the reality, immediacy, and scale of the threat. It is one well-recognized by states. The May 2010 U.S. National Security Strategy cites cyber security threats as "one of the most serious national security, public safety, and economic challenges we face as a nation."[6] Similarly, the analysis and recommendations on NATO's new Strategic Concept prepared by a group of distinguished experts led by former U.S. Secretary of State Madeleine Albright singled out "cyber assaults of varying degrees of severity" as one of the three likeliest threats the NATO Allies will face in the next decade.[7]

Unfortunately, the existing legal norms do not offer a clear and comprehensive framework within which states can shape policy responses to the threat of hostile cyber operations. In particular, international law as traditionally understood departs at times from what the international community would presumably demand in the cyber context. To some extent, this divergence can be accommodated through reasonable interpretation of the relevant norms. Where it cannot, the law would seem to require attention, either through treaty action or through the development of new understandings of the prevailing legal concepts.[8]

II. CYBER OPERATIONS AS A "USE OF FORCE"

The United Nations Charter, in Article 2(4), states that "[a]ll Members [of the United Nations] 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." Despite the reference to territorial integrity and political independence, it is now widely understood that the prohibition applies to any use of force not otherwise permitted by the terms of the Charter, specifically uses of force authorized by the Security Council and defensive operations, each discussed separately below.[9]

5. *See* TIKK ET AL., *supra* note 2, at 66-90 (describing cyber attacks against Georgia during dispute with Russia over South Ossetia).

6. THE WHITE HOUSE, NATIONAL SECURITY STRATEGY 27 (2010) [hereinafter 2010 NATIONAL SECURITY STRATEGY], *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

7. *See* N. Atlantic Treaty Org. [NATO], *NATO 2020: Assured Security; Dynamic Engagement* 17 (May 17, 2010) [hereinafter *NATO 2020*], *available at* http://www.nato.int/strategic-concept/expertsreport.pdf. The others are an attack by a ballistic missile and strikes by international terrorist groups. *See id.* (listing most probable threats of coming decade).

8. For book length treatment of these issues, see INTERNATIONAL LAW STUDIES: COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW, *supra* note 1; THOMAS C. WINGFIELD, THE LAW OF INFORMATION CONFLICT: NATIONAL SECURITY LAW IN CYBERSPACE (2000); 64 A.F. L. REV. (2009) (dedicating edition to cyberlaw).

9. In its original form, the draft Charter contained no reference to territorial integrity or political independence, and their subsequent inclusion was controver-

Article 2(4) was revolutionary in its extension to threats. Of course, only those threats of a use of force that would otherwise be unlawful qualify.[10] For instance, threatening destructive defensive cyber attacks against another state's military infrastructure if that state unlawfully mounts cross-border operations would not breach the norm. However, threats of destructive cyber operations against another state's critical infrastructure unless that state cedes territory would do so.

The prohibition applies only to an explicit or implied communication of a threat; its essence is coercive effect. It does not reach actions which simply threaten the security of the target state, but which are not communicative in nature. Thus, the introduction into a state's cyber systems of vulnerabilities that are capable of destructive activation at some later date would not constitute a threat of the use of force unless their presence is known to the target state and the originating state exploits them for some coercive purpose.[11]

It is generally accepted that the prohibition on the threat or use of force represents customary international law.[12] Resultantly, it binds all states regardless of membership in the United Nations. Article 38 of the Statute of the International Court of Justice (ICJ) defines customary law as "general practice accepted as law."[13] It requires the coexistence of state practice and *opinio juris sive necessitatis*, a belief that the practice is engaged in, or refrained from, out of a sense of legal obligation (rather than practical or policy reasons).

Although simple in formulation, the norm is complex in substantive composition. It poses two key questions: "What is a use of force?" and "To whom does the prohibition apply?" Both bear heavily on the legality of cyber operations, which did not exist when the UN Charter was adopted by states in 1945. The difficulty of applying a legal provision that did not contemplate a particular type of operation is apparent.

Finally, it must be borne in mind that neither Article 2(4) nor its customary counterpart is remedial in nature. Rather, they merely set a threshold for breach of international law. The nature of the response to a

---

sial. The "other manner" language was inserted to make clear that their inclusion was not meant to limit the reach of the provision. *See* Doc. 1123, I/8, 6 U.N.C.I.O. Docs. 65 (1945); Doc. 885, I/1/34, 6 U.N.C.I.O. Docs. 387 (1945); Doc. 784, I/1/27, 6 U.N.C.I.O. Docs. 336 (1945).

10. This point was made by the International Court of Justice in *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1996 I.C.J. 226, ¶ 47 (July 8) ("[I]f the use of force itself in a given case is illegal—for whatever reason—the threat to use such force will likewise be illegal.").

11. Although a threat must be coercive in some sense, there is no requirement that a specific "demand" accompany the threat.

12. *See* Military and Paramilitary Activities in and Against Nicaragua (*Nicaragua*) (Nicar. v. U.S.), 1986 I.C.J. 14, 98-101 (June 27).

13. Statute of the International Court of Justice, art. 38, 1977 I.C.J. Acts & Docs. 61. On customary law, see Yoram Dinstein, *The Interaction Between Customary International Law and Treaties, in* 322 Collected Courses of the Hague Academy of International Law 243 (2006).

wrongful use of force is instead determined by the law of state responsibility, the scope of authority of the Security Council, and the law of self-defense. Each is addressed below.

A. *Uses of Force*

Do cyber operations constitute a "use of force" as that phrase is understood in relation to the prohibition? The interpretive dilemma is that the drafters of the Charter took a cognitive shortcut by framing the treaty's prohibition in terms of the *instrument* of coercion employed—force. Thus, the norm did not outlaw economic and political coercion, but disallowed military force, at least absent an express Charter exception. Yet, it is seldom the instrument employed, but instead the *consequences* suffered, that matter to states. At the time the Charter was drafted an instrument based-approach made sense, for prior to the advent of cyber operations the consequences that states sought to avoid usually comported with instrument-based categories. Cyber operations do not fit neatly into this paradigm because although they are "non-forceful" (that is, non-kinetic), their consequences can range from mere annoyance to death. Resultantly, as the Commander of U.S. Cyber Command noted during his confirmation hearings, policy makers must understand that "[t]here is no international consensus on a precise definition of a use of force, in or out of cyberspace. Consequently, individual nations may assert different definitions, and may apply different thresholds for what constitutes a use of force."[14]

That the term "use of force" encompasses resort to armed force by a state, especially force levied by the military is self-evident. Armed force thus includes kinetic force—dropping bombs, firing artillery, and so forth. It would be no less absurd to suggest that cyber operations that generate consequences analogous to those caused by kinetic force lie beyond the prohibition's reach, than to exclude other destructive non-kinetic actions, such as biological or radiological warfare. Accordingly, cyber operations that directly result (or are likely to result) in physical harm to individuals or tangible objects equate to armed force, and are therefore uses of force. For instance, those targeting an air traffic control system or a water treatment facility clearly endanger individuals and property. But cyber operations are usually mounted without causing such consequences, as illustrated by the case of Estonia. Are such operations nonetheless barred by the use-of-force prohibition?

The starting point for any interpretive endeavor in law is the treaty text in question.[15] In this regard, note that the adjective "armed" does not

14. Staff of S. Comm. on Armed Services, Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command from the United States' Armed Services Committee (Apr. 15, 2010), www.senate.gov/~armed_services/statemnt/2010/04%20April/Alexander%2004-15-10.pdf.

15. According to the Vienna Convention on the Law of Treaties, "[a] treaty shall be interpreted in good faith in accordance with the ordinary meaning to be

appear with reference to "force" in Article 2(4). By contrast, the Charter preamble cites the purpose of ensuring that "armed force shall not be used, save in the common interest." Similarly, the Charter excludes "armed force" from the non-forceful measures the Security Council may authorize under Article 41 and mentions planning for armed force with regard to forceful Article 42 measures.[16] And the Charter only allows forceful defensive actions in the face of an "armed attack."[17] This textual distinction suggests an interpretation of "force" that is broader in scope than the common understanding of the term.

When text is ambiguous, recourse may be had to "the preparatory work of [a] treaty and the circumstances of its conclusion."[18] The Charter's *travaux preparatoires* indicate that during the drafting of the instrument a proposal to extend the reach of Article 2(4) to economic coercion was decisively defeated.[19] A quarter century later, the issue again arose during proceedings leading to the UN General Assembly's Declaration on Friendly Relations.[20] The question of whether "force" included "all forms of pressure, including those of a political or economic character, which have the effect of threatening the territorial integrity or political independence of any State" was answered in the negative.[21] Whatever force is, then, it is not economic or political pressure. Therefore, a cyber operation that involves such coercion is definitely not a prohibited use of force. Psychological cyber operations (assuming they are non-destructive) intended solely to undermine confidence in a government or economy illustrate such actions.

---

given to the terms of the treaty in their context and in light of its object and purpose" which can be gleaned from the text, "including its *preamble* and annexes . . . ." Vienna Convention on the Law of Treaties, art. 31(1)-(2), May 23, 1969, 1155 U.N.T.S. 331, 340 (emphasis added). The United States is not a party to the Vienna Convention, but treats most of its provisions as reflective of customary international law.

16. *See* U.N. Charter art. 46 (referencing planning for armed force). "Plans for the application of armed force shall be made by the Security Council with the assistance of the Military Staff Committee." *Id.*

17. U.N. Charter art. 51.

18. Vienna Convention on the Law of Treaties, *supra* note 15, art. 32, 1155 U.N.T.S. at 340.

19. *See* Doc. 2, G/7(e)(4), 3 U.N.C.I.O. Docs. 251, 253-54 (1945). Economic coercion, which typically involves trade sanctions, must be distinguished from "blockade," which has the effect of cutting off trade, but employs military force to do so. It has historically been accepted that imposition of a blockade is an "act of war."

20. *See* Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625 (XXV), U.N. GAOR, 25th Sess., Supp. No. 28, U.N. Doc. A/RES/8082 (Oct. 24, 1970).

21. U.N. GAOR Special Comm. on Friendly Relations, U.N. Doc. A/AC.125/SR.114 (1970); *accord* Rep. of the Special Comm. on Principles of Int'l Law Concerning Friendly Relations and Co-operation Among States, U.N. GAOR, 24th Sess., Supp. No. 19, U.N. Doc. A/7619 (1969). The draft declaration contained text tracking that of U.N. Charter Article 2(4).

Suggestions to limit "force" to "armed force," or even the force required to amount to an "armed attack," were likewise rejected during the proceedings.[22] This seemed to indicate that "force" was not coterminous with "armed force," thereby strengthening the significance of the absence of the term "armed" in Article 2(4). In the *Case Concerning Military and Paramilitary Activities in and Against Nicaragua*,[23] the ICJ expressly characterized certain actions that were non-kinetic in nature as uses of force:

> [W]hile the arming and training of the contras can certainly be said to involve the threat or use of force against Nicaragua, this is not necessarily so in respect of all the assistance given by the United States Government. In particular, the Court considers that the mere supply of funds to the contras, while undoubtedly an act of intervention in the internal affairs of Nicaragua . . . does not in itself amount to a use of force.[24]

The determination that a use of force can embrace acts, like arming or training guerillas, which fall short of armed force leaves open the possibility that non-physically destructive cyber operations may fall within the term's ambit. The threshold for a use of force must therefore lie somewhere along the continuum between economic and political coercion on the one hand and acts which cause physical harm on the other.

Unfortunately, unequivocal state practice in characterizing particular cyber attacks as (or not as) uses of force is lacking. In part, this is because the Article 2(4) prohibition extends solely to acts of states, and very few states have definitively been identified as the initiator of a cyber operation that might amount to a use of force. Moreover, states may well hesitate to label a cyber operation as a use of force out of concern that doing so would escalate matters or otherwise destabilize the situation. Therefore, one can only speculate as to future state practice regarding the characterization of cyber operations.

Over a decade ago, this author identified a number of factors that would likely influence assessments by states as to whether particular cyber operations amounted to a use of force.[25] They are based on a recognition that while states generally want to preserve their freedom of action (a motivation to keep the threshold high), they equally want to avoid any harmful consequences caused by the actions of others (a motivation to keep the threshold low). Thus, states will seek to balance these conflicting objectives through consideration of factors such as those set forth below. The approach has generally withstood the test of time.

---

22. *See* U.N. GAOR Special Comm. on Friendly Relations, U.N. Doc. A/AC.125/SR.114 (1970).

23. *Nicaragua* (Nicar. v. U.S.), 1986 I.C.J. 14 (June 27).

24. *Id.* ¶ 228.

25. *See* Michael N. Schmitt, *Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 914-16 (1999).

1) *Severity*: Consequences involving physical harm to individuals or property will alone amount to a use of force. Those generating only minor inconvenience or irritation will never do so. Between the extremes, the more consequences impinge on critical national interests, the more they will contribute to the depiction of a cyber operation as a use of force. In this regard, the scale, scope, and duration of the consequences will have great bearing on the appraisal of their severity. Severity is self-evidently the most significant factor in the analysis.

2) *Immediacy*: The sooner consequences manifest, the less opportunity states have to seek peaceful accommodation of a dispute or to otherwise forestall their harmful effects. Therefore, states harbor a greater concern about immediate consequences than those that are delayed or build slowly over time.

3) *Directness*: The greater the attenuation between the initial act and the resulting consequences, the less likely states will be to deem the actor responsible for violating the prohibition on the use of force. Whereas the immediacy factor focused on the temporal aspect of the consequences in question, directness examines the chain of causation. For instance, the eventual consequences of economic coercion (economic downturn) are determined by market forces, access to markets, and so forth. The causal connection between the initial acts and their effects tends to be indirect. In armed actions, by contrast, cause and effect are closely related—an explosion, for example, directly harms people or objects.

4) *Invasiveness*: The more secure a targeted system, the greater the concern as to its penetration. By way of illustration, economic coercion may involve no intrusion at all (trade with the target state is simply cut off), whereas in combat the forces of one state cross into another in violation of its sovereignty. The former is undeniably not a use of force, whereas the latter always qualifies as such (absent legal justification, such as evacuation of nationals abroad during times of unrest). In the cyber context, this factor must be cautiously applied. In particular, cyber exploitation is a pervasive tool of modern espionage. Although highly invasive, espionage does not constitute a use of force (or armed attack) under international law absent a nonconsensual physical penetration of the target state's territory, as in the case of a warship or military aircraft which collects intelligence from within its territorial sea or airspace. Thus, actions such as disabling cyber security mechanisms to monitor keystrokes would, despite their invasiveness, be unlikely to be seen as a use of force.

5) *Measurability*: The more quantifiable and identifiable a set of consequences, the more a state's interest will be deemed to have been affected. On the one hand, international law does not view economic coercion as a use of force even though it may cause significant suffering. On the other, a military attack that causes only a limited degree of destruction clearly qualifies. It is difficult to identify or quantify the harm caused

by the former (e.g., economic opportunity costs), while doing so is straightforward in the latter (X deaths, Y buildings destroyed, etc).

6) *Presumptive legitimacy*: At the risk of oversimplification, international law is generally prohibitory in nature. In other words, acts which are not forbidden are permitted; absent an express prohibition, an act is presumptively legitimate.[26] For instance, it is well accepted that the international law governing the use of force does not prohibit propaganda, psychological warfare, or espionage. To the extent such activities are conducted through cyber operations, they are presumptively legitimate.

7) *Responsibility*: The law of state responsibility (discussed below) governs when a state will be responsible for cyber operations. But it must be understood that responsibility lies along a continuum from operations conducted by a state itself to those in which it is merely involved in some fashion. The closer the nexus between a state and the operations, the more likely other states will be inclined to characterize them as uses of force, for the greater the risk posed to international stability.

The case of the Estonian cyber attacks can be used to illustrate application of the approach. Although they caused no deaths, injury, or physical damage, the attacks fundamentally affected the operation of the entire Estonian society. Government functions and services were severely disrupted, the economy was thrown into turmoil, and daily life for the Estonian people was negatively affected. The consequences far exceeded mere inconvenience or irritation. The effects were immediate and, in the case of confidence in government and economic activity, wide-spread and long-term. They were also direct, as with the inability to access funds and interference with the distribution of government benefits. Since some of the targeted systems were designed to be secure, the operations were highly invasive. While the consequences were severe, they were difficult to quantify, since most involved denial of service, rather than destruction of data. Although political and economic actions are presumptively legitimate in use-of-force terms, these operations constituted more than merely pressuring the target state. Instead, they involved intentionally frustrating governmental and economic functions. Taken together as a single "cyber operation," the incident arguably reached the use-of-force threshold. Had Russia been responsible for them under international law, it is likely that the international community would have (or should have) treated them as a use of force in violation of the UN Charter and customary international law.

---

26. In *The Case of the S.S. "Lotus"*, the Permanent Court of International Justice famously asserted that "[t]he rules of law binding upon States . . . emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims." S.S. "Lotus" (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 18 (Sept. 7).

The criteria are admittedly imprecise, thereby permitting states significant latitude in characterizing a cyber operation as a use of force, or not. In light of the increasing frequency and severity of cyber operations, a tendency towards resolving grey areas in favor of finding a use of force can be expected to emerge. This state practice will over time clarify the norm and its attendant threshold.

B. *Applicability of the Prohibition*

By its own express terms, Article 2(4) applies solely to Members of the United Nations. As discussed, the prohibition extends to non-Members by virtue of customary law. That is the limit of applicability. Non-state actors, including individuals, organized groups, and terrorist organizations, cannot violate the norm absent a clear relationship with a state. Their actions may be unlawful under international and domestic law, but not as a violation of the prohibition on the use of force. Thus, in the Estonian case, and barring any evidence of Russian government involvement, none of those individuals or groups conducting the operations violated the Article 2(4) prohibition. But when can the conduct of individuals or groups be attributed to a state, such that the state is legally responsible for their actions? The law of state responsibility governs such situations.[27]

Obviously, states are legally responsible for the conduct of their governmental organs or entities.[28] This principle extends to unauthorized acts.[29] Accordingly, any cyber operation rising to the level of an unlawful use of force will entail responsibility on the part of the state when launched by its agents, even when they are acting *ultra vires*.

The fact that a state did not itself conduct the cyber operations at hand does not mean that it escapes responsibility altogether. States are also responsible for "the conduct of a person or group of persons . . . if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."[30] The ICJ addressed the degree of control necessary for attribution in the *Nicaragua* case. There the Court considered attribution of the acts of the Nicaraguan Contras (a rebel group supported by the United States) to the United States, such that the United States would be responsible for breaches of international humanitarian law (IHL) committed by the group. While finding the United States responsible for its own "planning, direction and support" of the Contras,[31] the court limited responsibility

27. This law is set forth, in non-binding form, in the International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Acts, *in* Report of the Int'l Law Comm'n, 53d Sess., Apr. 23-June 1, July 2-Aug. 10, 2001, UN Doc. A/56/10; GAOR, 56th Sess., Supp. No. 10 (2001) [hereinafter Draft Articles on State Responsibility].

28. *See id.* art. 4, at 44.

29. *See id.* art. 7, at 44.

30. *See id.* art. 8, at 45.

31. *Nicaragua* (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 86 (June 27).

for the Contra actions to those in which the United States exercised "*effective control* of the military or paramilitary operations in the course of which the alleged violations were committed."[32] Mere support for their activities did not suffice.

The Appeals Chamber of the International Criminal Tribunal for the Former Yugoslavia (ICTY) took a different tack in the *Prosecutor v. Tadic*[33] case, where it held that the authority of the government of the Federal Republic of Yugoslavia over the Bosnia Serb armed groups "required by international law for considering the armed conflict to be international was *overall control* going beyond the mere financing and equipping of such forces and involving also participation in the planning and supervision of military operations."[34] It is essential to note that although the tribunal expressly rejected the higher *Nicaragua* threshold of effective control, the technical legal issue was not state responsibility, but rather the nature of the armed conflict. Thus, while *Tadic* brings *Nicaragua* into question by proffering a lower threshold, it does not necessarily supplant the effective control test.[35] It remains unclear whether effective control, overall control, or some other test governs in international law, although the ICJ has twice reaffirmed its version.[36]

In the cyber context, then, states will be responsible for violating the prohibition on the use of force to the extent that they either direct private individuals or groups to conduct the operations or are heavily involved in them. Determinations will be made on a case-by-case basis by looking to the extent and nature of involvement by the state with the group and in the particular operations.

Even if conduct is not attributable to a state as under its control, it will nevertheless "be considered an act of that State . . . if and to the extent that the State acknowledges and adopts the conduct in question as its own."[37] The ICJ addressed this situation in the *Case Concerning United States Diplomatic and Consular Staff in Tehran*,[38] which involved seizure of the U.S. Embassy by Iranian militants in 1979. The Iranian government was uninvolved in the initial seizure, but later passed a decree that accepted and maintained the occupation of the embassy. According to the ICJ, "[t]he approval given to [the occupation of the Embassy] by the

32. *Id.* ¶ 115 (emphasis added); *id.* ¶ 109.

33. Prosecutor v. Tadic, Case No. IT-94-1-A, Appeals Chamber Judgment (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).

34. *Id.* ¶ 145.

35. Although, the court in dicta suggested the test is also suitable for application to issues of state responsibility. *See id.*, ¶¶ 116-37.

36. *See, e.g.*, Application of Convention on Prevention and Punishment of Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 91, 391-92 (Feb. 26); Armed Activities on the Territory of the Congo (*Congo*) (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, ¶ 160 (Dec. 19).

37. Draft Articles on State Responsibility, *supra* note 27, art. 11, at 45.

38. United States Diplomatic and Consular Staff in Teheran (U.S. v. Iran), 1980 I.C.J. 3 (May 24).

Ayatollah Khomeini and other organs of the Iranian State, and the decision to perpetuate them, translated continuing occupation of the Embassy and detention of the hostages into acts of that State."[39]

It should be cautioned that mere expressions of approval do not suffice for attribution; rather, the state must somehow subsequently embrace the actions as its own, for instance, by tangibly supporting their continuance, failing to take actions to suppress them, or otherwise adopting them. Adoption may either be express, as in the *Hostages* case, or implied, as when a state engages in conduct that undeniably constitutes adoption. In the Estonian case, had Russia publicly encouraged further attacks, it would have borne responsibility not only for the subsequent attacks, but also those in the initial wave.

A state may also be held responsible for the effects of unlawful acts of private individuals or groups on its territory when it fails to take reasonably available measures to stop such acts in breach of its obligations to other states. In this situation, its violation is of the duty owed to other states, but its responsibility extends to the effects of the act itself. Applying this standard in the *Hostages* case, the ICJ found that the Iranian government failed to take required steps to prevent the seizure of the U.S. Embassy or regain control over it, placing Iran in breach of its international obligation to safeguard diplomatic premises.[40] The key to such responsibility lies in the existence of a separate legal duty to forestall the act in question, and an ability to comply with said duty. The ICJ articulated this principle in its very first case, *Corfu Channel*,[41] where it held that every state has an "obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[42] Of the many obligations that states owe to each other, ensuring their territory is not a launching pad for the use of force or armed attacks (see discussion below) against other states certainly ranks among the most important. The fact that a use of force consists of cyber operations rather than traditional armed force would not diminish the responsibility of the state involved.

Finally, consider a situation in which the effects of a cyber operation extend beyond the targeted state. This is an especially relevant scenario in the cyber context, for networking and other forms of interconnectivity mean that a cyber use of force by State A against State B may have consequences in State C that would rise to the level of a use of force if directed against C. The causation of such effects would not amount to a violation of Article 2(4) vis-à-vis C. Article 2(4)'s requirement that Members "refrain in their international *relations*"[43] from the use of force implies an element of purposely engaging in some action in respect of another speci-

39. *Id.* ¶ 74.

40. *See id.* ¶¶ 76-78.

41. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4 (Apr. 9).

42. *Id.* at 22.

43. U.N. Charter art. 2(4) (emphasis added).

fied state. Inadvertent effects caused in states other than the target state do not constitute a form of "international relations."

However, even if the state did not intend such effects, it is clear that it bears responsibility for them. As noted in the Draft Articles of State Responsibility, "[t]here is an internationally wrongful act of a State when conduct consisting of an action or omission: (a) [i]s attributable to the State under international law; and (b) [c]onstitutes a breach of an international obligation of the State."[44] In the envisaged case, since State A conducted the cyber operation, the action is directly attributable to it. Further, the wrongful use of force against B would constitute a breach of A's international obligation to refrain from the use of force. That the intended "victim" was B matters not. The criterion has been met once the breach of an international obligation has occurred. This is so even if the effects in C were unintended. As noted in the International Law Commission's Commentary to the relevant article:

> A related question is whether fault constitutes a necessary element of the internationally wrongful act of a State. This is certainly not the case if by "fault" one understands the existence, for example, of an intention to harm. In the absence of any specific requirement of a mental element in terms of the primary obligation, it is only the act of a State that matters, independently of any intention.[45]

C. *Remedies for Violation*

In the event of state responsibility for an unlawful act, the victim-state is entitled to reparation, which can take the form of restitution, compensation, or satisfaction.[46] With regard to cyber operations amounting to a use of force, compensation could be claimed for any reasonably foreseeable physical or financial losses. A state may also take any responsive actions that neither amount to a use of force nor breach an existing treaty or customary law obligation. As an example, a state may choose to block incoming cyber transmissions emanating from the state that has used force against it.

---

44. Draft Articles of State Responsibility, *supra* note 27, art. 2, at 43.

45. JAMES CRAWFORD, THE INTERNATIONAL LAW COMMISSION'S ARTICLES ON STATE RESPONSIBILITY: INTRODUCTION, TEXT AND COMMENTARIES 84 (2002).

46. *See* Draft Articles on State Responsibility, *supra* note 27, arts. 34-37, at 52. Restitution is reestablishing "the situation which existed before the wrongful act was committed." *Id.* art. 35, at 52. Compensation is covering any financially assessable damage not made good by restitution. *See id.* art. 36, at 52. Satisfaction is "an acknowledgement of the breach, an expression of regret, a formal apology or another appropriate modality" that responds to shortfalls in restitution and compensation when making good the injury caused. *Id.* art. 37, at 52.

Additionally, the victim-state may take "countermeasures" in response to a use of force.[47] Countermeasures are "measures which would otherwise be contrary to the international obligations of the injured State *vis-à-vis* the responsible State if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation."[48] They are distinguished from retorsion, which is the taking of unfriendly but lawful actions, such as the expulsion of diplomats.

The wrong in question has to be on-going at the time of the countermeasures, since their purpose is not to punish or provide retribution, but instead to compel the other party to desist in its unlawful activities.[49] Countermeasures must be proportionate to the injury suffered,[50] and the victim-state is required to have called on the state committing the wrong to refrain from the conduct (and make reparations if necessary), or, in the case of acts emanating from its territory, take measures to stop them.[51] Unlike collective self-defense (discussed below), countermeasures may only be taken by the state suffering the wrong.[52]

Countermeasures involving cyber operations would be particularly appropriate as a response to a cyber use of force, although the strict limitations placed on countermeasures weaken their viability in situations demanding an immediate reaction. On the other hand, it would be improper to respond with a cyber operation that rose to the level of a use of force, for "[c]ountermeasures shall not affect . . . the obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations."[53] Responses amounting to a use of force are only permissible when falling within the two recognized exceptions to the prohibition on the use of force—action authorized by the Security Council and self-defense.

Although the limitation of countermeasures to non-forceful measures is widely accepted, in a separate opinion to the ICJ's *Case Concerning Oil Platforms*[54] judgment, Judge Simma argued for what might be labeled "self-defense lite" in the face of an "unlawful use of force 'short of' an armed attack . . . within the meaning of Article 51."[55] For Judge Simma, such "defensive military action 'short of' full scale self-defence" is of a "more limited range and quality of response" than that which is lawful in re-

47. *See id.* art. 49(1), at 56; *see also* Gabcikovo-Nagymaros Project (Hung. v. Slovk.) 1997 I.C.J. 7, 55-56 (Sept. 25); *Nicaragua* (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 249 (June 27).

48. Report of the Int'l Law Comm'n, *supra* note 27, at 324.

49. *See* Draft Articles on State Responsibility, *supra* note 27, art. 52(3)(a), at 57-58.

50. *See id.* art. 51, at 57.

51. *See id.* art. 52(1), at 57.

52. *See Nicaragua* (Nicar. v. U.S.), *1986 I.C.J. 14*, ¶¶ 211, 252.

53. Draft Articles on State Responsibility, *supra* note 27, art. 50(1)(a), at 57.

54. *Oil Platforms* (Iran v. U.S.), 2003 I.C.J. 161 (Nov. 6).

55. *Id.* at 331 (separate opinion of Judge Simma).

sponse to an armed attack in the self-defense context. The key difference with classic self-defense is that Judge Simma would exclude collective actions.[56] Reduced to basics, he is arguing for normative acceptance of forceful countermeasures.

The core problem with the approach is that it posits a tiered forceful response scheme. However, because the intensity of a defensive response is already governed, as will be discussed below, by the principle of proportionality, all that is really occurring is a relaxation of the threshold for engaging in forceful defensive actions. Such an approach is counter-textual, for the combined effect of Articles 2(4) and 51 of the UN Charter is to rule out forcible responses by states against actions other than "armed attacks." Nevertheless, acceptance of such an approach by states would be significant in the cyber context because by it cyber operations, which themselves would be a use of force under Article 2(4), may be launched in reaction to a cyber use of force that did not rise to the level of an armed attack under Article 51.

III. AUTHORIZATION BY THE SECURITY COUNCIL

Pursuant to Article 39 of the UN Charter, the Security Council is empowered to determine that a particular situation amounts to a "threat to the peace, breach of the peace or act of aggression." When it does, the Council "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." Articles 41 and 42 set forth, respectively, non-forceful and forceful options for responding to such situations.

The scope of the phrase "threat to the peace, breach of the peace or act of aggression" has been the subject of much attention in international law. Breach of the peace would seemingly require the outbreak of violence; cyber operations harming individuals or property would reasonably qualify, but whether those falling short of this level would do so is uncertain. As to aggression, in 1974 the General Assembly adopted a resolution in which it characterized "aggression" as ranging from the "use of armed force" and blockade to allowing one's territory to be used by another state to commit an act of aggression and sending armed bands against another state.[57] A cyber operation causing significant physical harm in another state would certainly rise to this level; whether others would is unclear.

This ambiguity is essentially irrelevant in light of the "threat to the peace" criterion. Little guidance exists on those acts which qualify, although they must be conceptually distinguished from activities constituting threats of the use of force in contravention of Article 2(4). In *Tadic*, the ICTY opined that a threat to the peace should be assessed with regard to the Purposes of the United Nations delineated in Article 1 and the Prin-

56. *See id.* at 331-33.

57. Definition of Aggression, G.A. Res. 3314 (XXIX), Annex art. 3, U.N. DOC. A/RES/3314 (Dec. 14, 1974).

ciples set forth in Article 2.[58] This is a singularly unhelpful proposition, since said Purposes and Principles include such intangibles as developing friendly relations and solving social problems.

In fact, a finding that a situation is a threat to the peace is a political decision, not a legal one. It signals the Security Council's willingness to involve itself in a particular matter. There are no territorial limits on situations which may constitute threats to the peace, although they logically tend to be viewed as those which transcend borders, or risk doing so. Nor is there a limitation to acts conducted by or at the behest of states; for instance, the Council has repeatedly found transnational terrorism to be a threat to the peace.[59] No violence or other harmful act need have occurred before the Council may make a threat to the peace determination. Most importantly, since there is no mechanism for reviewing threat to the peace determinations, the Council's authority in this regard is unfettered. Simply put, a threat to the peace is whatever the Council deems it to be. This being so, the Council may label any cyber operation a threat to the peace (or breach of peace or act of aggression), no matter how insignificant.

Once it does, the Security Council may, under Article 41, authorize measures "not involving the use of armed force" necessary to maintain or restore international peace and security. Article 41 offers a number of examples, including "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio or other means of communication." Interruption of cyber communications would necessarily be included. An interruption could be broad in scope, as in blocking cyber traffic to or from a country, or surgical, as in denying a particular group access to the Internet. Any other cyber operations judged necessary would likewise be permissible. Given the qualifier "armed force," operations resulting in physical harm to persons or objects could not be authorized pursuant to Article 41.

Should the Council determine that Article 41 measures are proving ineffective, or if before authorizing them it decides that such measures would be fruitless, it may, pursuant to Article 42, "take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security." The reference to operations by "air, sea, or land forces" plainly contemplates forceful military action, although a Security Council resolution authorizing the use of force will typically be framed in

58. *See* Prosecutor v. Tadic, Case No. IT-94-1-I, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 29 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

59. *See, e.g.*, S.C. Res. 1618, U.N. Doc. S/RES/1618 (Aug. 4, 2005); S.C. Res. 1611, U.N. Doc. S/RES/1611 (July 7, 2005); S.C. Res. 1530, U.N. Doc. S/RES/1530 (Mar. 11, 2004); S.C. Res. 1516, U.N. Doc. S/RES/1516 (Nov. 20, 2003); S.C. Res. 1465, U.N. Doc. S/RES/1465 (Feb. 13, 2003); S.C. Res. 1450, U.N. Doc. S/RES/1450 (Dec. 13, 2002); S.C. Res. 1440, U.N. Doc. S/RES/1440 (Oct. 24, 2002); S.C. Res. 1438, U.N. Doc. S/RES/1438 (Oct. 14, 2002); S.C. Res. 1377, U.N. Doc. S/RES/1377 (Nov. 12, 2001).

terms of taking "all necessary measures." To the extent that military force can be authorized, it is self-evident that cyber operations may be as well. It would be lawful to launch them alone or as an aspect of a broader traditional military operation. The sole limiting factors would be the requirement to comply with other norms of international law, such as the IHL prohibition on attacking the civilian population,[60] and the requirement to restrict operations to those within the scope of the particular authorization or mandate issued by the Council. Article 42 actions are not limited territorially or with regard to the subject of the sanctions. For example, it would undoubtedly be within the power of the Council to authorize cyber attacks against transnational terrorist groups (e.g., in order to disrupt logistics or command and control). It is important to emphasize that the measures only extend to restoring peace if breached, or maintaining it when threatened. No authority exists for taking punitive measures.

Pursuant to Article 25 of the Charter, UN Members "agree to accept and carry out the decisions of the Security Council in accordance with the present Charter." This obligation applies even in the face of conflicting domestic or international legal obligations.[61] Consequently, if the Council ordered restrictions, for example, on cyber communications, individual states would be obligated to abide by them and ensure, to the extent feasible, their enforcement on their territory. How they do so is not the concern of the Council, so long as its decision is respected.

Since the United Nations does not itself control cyber networks or have the capability to mount cyber operations, it would have to rely on states to effectuate any cyber related resolutions. Originally, it was envisioned that the Security Council would have dedicated forces at its disposal to conduct Article 42 operations pursuant to "special agreements" with contributing countries.[62] Such arrangements have never been executed. The Council has instead relied upon authorizations granted to individual states, ad hoc coalitions of states, security organizations such as NATO, or UN forces consisting of troop contributions from its Members. State practice has established that no obligation exists for states to provide military forces or finance specific operations that have been authorized. Therefore, if the Council were to endorse specific defensive or offensive cyber operations under Article 42, it would be wholly dependent on the willingness of states to provide the necessary cyber assets and forces to execute them.

Finally, it must be recalled that the entire UN collective security system depends on the readiness of the five Permanent Members of the Security Council (P5) to allow for action by refraining from exercise of their

60. *See* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts arts. 48, 51, 52, June 8, 1977, 1125 U.N.T.S. 3, 25-27 [hereinafter AP I].

61. *See* U.N. Charter art. 103.

62. *Id.* art. 43.

veto right.[63] In light of Russia's and China's presence on the Council (cyber operations regularly emanate from their territory), this limitation may well prove the greatest obstacle to effective UN action in the face of those cyber operations which would in some fashion endanger international stability.

IV. SELF-DEFENSE

The second recognized exception to the prohibition on the use of force is the right of states to take forceful actions to defend themselves. This customary international law right is codified in Article 51 of the UN Charter. In relevant part, it provides that "[n]othing 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 measures necessary to maintain international peace and security." The article is the *conditio sine qua non* of the Charter, for although Articles 41 and 42 provide Member States some degree of protection from attack, their provisions rely upon implementation by the Security Council. Article 51 represents an essential safeguard in the event the collective security mechanism fails (or proves insufficiently timely), for it provides a means of defense requiring no Security Council approval. In practice, the right of self-defense has proven the principal means by which states ensure their security.

The right of self-defense bears solely on the remedies available to the victim of an armed attack, since all such attacks are "uses of force" in the context of Article 2(4) and customary law, with their legality determined by reference to those norms. By contrast, the issue in self-defense is the lawfulness of a forceful defensive response (including its nature, intensity, duration, and scope) that would otherwise constitute an unlawful use of force by a state. This being so, it has no bearing on passive cyber defenses, which merely block attacks; all such defenses are lawful. It is only in the case of active defenses, whether kinetic or cyber in nature, that the law of self-defense comes into play by directly imposing physical costs on the group or state launching an attack.[64]

Further, states alone enjoy the right of self-defense. Private entities, such as a corporation that has been subjected to a hostile cyber attack, cannot respond pursuant to the law of self-defense regardless of its severity. Their responses would be governed by domestic and international criminal law norms. However, cyber attacks against a state's nationals may

63. *See id.* art. 27(3).

64. Note that one of the recommendations of the experts in the *NATO 2020* report was that "NATO should plan to mount a fully adequate array of cyber defence capabilities, including passive and active elements." *NATO 2020*, *supra* note 7, at 45. It should be noted, however, that passive defenses must nevertheless comport with other aspects of international law. *See, e.g.*, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (*Wall*), Advisory Opinion, 2004 I.C.J. 136 (July 9).

sometimes qualify as an armed attack on the state itself; there is no requirement in international law that state property or organizations be targeted. In such a case, the state may respond forcefully in self-defense should it choose to do so.

A. *Armed Attack*

The key text in Article 51, and the foundational concept of the customary law right of self-defense, is "armed attack." But for an armed attack, states enjoy no right to respond forcefully to a cyber operation directed against them, even if that operation amounts to an unlawful use of force. This dichotomy was intentional, for it comports with the general presumption permeating the Charter scheme against the use of force, especially unilateral action. In the *Nicaragua* case, the ICJ acknowledged the existence of this gap between the notions of use of force and armed attack when it recognized that there are "measures which do not constitute an armed attack but may nevertheless involve a use of force" and distinguished "the most grave forms of the use of force from other less grave forms."[65] Recall that the court specifically excluded the supply of weapons and logistical support to rebels from the ambit of armed attack, but noted that such actions might constitute uses of force.[66] Simply put, all armed attacks are uses of force, but not all uses of force qualify as armed attacks.

As a result of the gap, the remedies for a use of force not meeting the threshold of armed attack are limited to lawful, non-forceful actions and countermeasures or recourse to the Security Council. What this means in practical terms is that, absent Security Council authorization, a state subjected to a use of force may not respond in kind unless the use of force rises to the level of an armed attack. In light of the difficulties of identifying the source of a cyber operation, this cautious two-tiered system is especially appropriate in the cyber context. It is important to emphasize, however, that once it is established that an armed attack has occurred, no authorization from the Security Council is necessary before defensive actions, including those involving destructive cyber operations, may be mounted.

Consistent with the use of force prohibition, the Charter drafters elected an instrument-based approach to articulating the right of self-defense. And as with that norm, the intent was to preclude certain consequences (in this case, a premature forceful reaction by a state threatened with harm that would itself threaten community stability), while nevertheless allowing states to react forcefully when the consequences justified as much. But, again, the possibility of devastating consequences caused by a non-kinetic cyber attack was obviously not considered during the drafting

65. *Nicaragua* (Nicar. v. U.S.), 1986 I.C.J. 14, ¶¶ 191, 210 (June 27); *accord Oil Platforms* (Iran v. U.S.), 2003 I.C.J. 161, 186-87 (Nov. 6).

66. *Nicaragua*, 1986 I.C.J. 14, ¶ 195.

process. Had it been, the drafters would surely have allowed for defense in the face of the severe consequences that can be caused by such attacks.

There is a problem in extending the notion of armed attack to address cyber attack operations of this magnitude. The facts that the use of force language in Article 2(4) is not qualified by the term "armed" and that the phrase "use of force" has been authoritatively interpreted as not necessarily implying a kinetic action allow for interpretive leeway, and the resulting application of the seven factors set forth above. By contrast, the phrase "armed attack" tolerates little interpretive latitude.

Clearly, an armed attack includes kinetic military force. Applying the consequence-based approach, armed attack must also be understood in terms of the effects typically associated with the term "armed." The essence of an armed operation is the causation, or risk thereof, of death of or injury to persons or damage to or destruction of property and other tangible objects. Therefore, while an armed attack need not be carried out through the instrument of classic military force, its consequences (or likely consequences but for successful defensive action) must be analogous to those resulting from its employment. A cyber operation that does not risk these results may qualify as an unlawful use of force, but will not comprise an armed attack permitting forceful defensive action.

In light of the grave consequences that cyber operations can cause without physically harming persons or objects, this interpretation may seem wholly unsatisfactory. Nevertheless, it is the extant law. It must be acknowledged that states victimized by massive cyber attacks, similar to or more aggravated than those suffered by Estonia, may choose to treat them as justifying a forceful response. If state practice along these lines became widespread and well-accepted, the Article 51 norm would shift accordingly through the natural process by which existing international law remains current. For the moment, that has not occurred.

Cyber operations that accompany military action otherwise constituting an armed attack have no bearing on the nature of the attack. For instance, cyber attacks would likely be conducted against enemy command and control or air defense systems as an element of a broader military operation. They can be responded to forcefully, regardless of whether they independently qualify as an armed attack, because they are a component of the overall military action. Similarly, cyber operations that are part of a lawful military response to an armed attack are obviously permissible so long as they comply with IHL, such as the prohibition on attacking civilians or civilian objects.[67] On the other hand, cyber operations need not accompany classic military operations. A cyber attack standing alone will comprise an armed attack when the consequence threshold is reached. Equally, states subjected to an armed attack may elect to respond solely with cyber operations.

67. *See* AP I, *supra* note 60, arts. 48, 51, 52, 1125 U.N.T.S. at 25-27.

In the *Nicaragua* case, the ICJ noted that not all attacks qualify as armed attacks, citing the case of "a mere frontier incident."[68] According to the court, an armed attack must exhibit certain "scale and effects." Unfortunately, the court failed to prescribe criteria by which to resolve whether an attack meets the armed attack threshold. Not only has this proposition been fairly criticized, but in the *Oil Platforms* case the court itself admitted that the mining of even a single ship could amount to an armed attack giving rise to the right of self-defense.[69] Consequently, by contemporary international law, qualitative indicators of attack (death, injury, damage, or destruction) are more reliable in identifying those actions likely to be characterized as an armed attack than quantitative ones (number of deaths or extent of destruction). So long as a cyber operation is likely to result in the requisite consequences, it is an armed attack.

With regard to cyber operations, it must be cautioned that the mere destruction or damage (alteration) of data would not suffice. Were it to, the armed attack threshold would be so reduced that the vast majority of cyber operations would qualify as armed attacks. Rather, to comport with the accepted understanding of "armed attack," the destruction of or damage to the data would have to result in physical consequences, as in causing a generator to overheat and catch fire or rendering a train or subway uncontrollable such that it crashed. Destruction of data designed to be immediately convertible into tangible objects, like banking data, could also be reasonably encompassed within the scope of "armed attacks." But the destruction of or damage to data, standing alone, would not rise to the level of an armed attack.

It is sometimes argued that a cyber operation directed against a nation's military capability necessarily constitutes an armed attack. If the attack is physically destructive, there is no question that this is so. But the mere fact that cyber operations "compromise the ability of units of the DOD to perform DOD's mission" does not alone suffice.[70] Only when non-destructive cyber operations indicate that an attack is imminent ("preparing the battlefield") or represent the first step in an attack that is underway (as in bringing down an air defense radar network to facilitate penetration of enemy airspace) are forceful actions in self-defense permissible. Obviously, it may be difficult to determine whether a particular cyber operation against military assets is either an indication or a component of attack; yet, that is a practical problem which does not affect the norm itself. As with the challenge of identifying an attacker or determin-

68. *Nicaragua* (Nicar v. U.S.), 1986 I.C.J. 14, ¶ 195.

69. *See Oil Platforms* (Iran v. U.S.), 2003 I.C.J. at 195-96; *see also* YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 194-96 (4th ed. 2005); William H. Taft IV, *Self-Defense and the* Oil Platforms *Decision*, 29 YALE J. INT'L L. 295, 300 (2004).

70. NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 245 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009).

ing when attack is imminent (discussed below), the legal issue is whether the defender's conclusion is reasonable in the circumstances.

Finally, a cyber use of force by State A against State B may generate "bleed-over" effects in State C. This situation does not, as noted earlier, constitute a use of force against C, although A would nevertheless be responsible for the consequences caused. However, if the effects in C rise to the level of those qualifying as an armed attack, C may respond in self-defense against State A, even though C was not the intended target of the attack.[71]

The distinction arises from the fact that while the use of force prohibition solely pertains to the issue of whether there has been a particular violation of international law, the law of self-defense addresses whether a victim-state enjoys the right to employ force to protect itself. It would be incongruous to suggest that a state was barred from acting defensively when subjected to such effects. From its perspective (the correct vantage point in interpreting the law of self-defense), what matters is deterring or stopping the harmful actions; the intention of the actor is but a secondary consideration. Of course, the defensive actions must meet the criteria of self-defense set forth below, in particular the requirement that a forceful response be "necessary." Because C was not the intended target of the attack, it may suffice to simply notify A that it is suffering effects from the attack on B and demand that A takes steps to arrest them.

B. *Anticipatory Self-Defense*

Textually, Article 51 addresses only those situations where an armed attack is underway. Nevertheless, it is well-accepted that a state need not sit idly by as the enemy prepares to attack; instead, a state may defend itself once attack is "imminent."[72] The generally accepted standard of imminency was articulated in the nineteenth century by Secretary of State

71. As the right of self-defense extends to armed attacks by non-state actors, an identical conclusion would apply to actions they undertake against one state having effects in another.

72. Acceptance of the standard is not universal. For instance, Professor Yoram Dinstein argues against its existence, suggesting instead that such actions are better seen as "interceptive self-defense." He notes that "an interceptive strike counters an armed attack which is in progress, even if it is still incipient: the blow is 'imminent' and practically 'unavoidable.'" DINSTEIN, *supra* note 69, at 191. It might also be noted that whereas the notion of *armed* attack was interpreted with fidelity to the Charter text, this article accepts an interpretation of self-defense which runs contrary to the precise text of the UN Charter. The apparent inconsistency can be justified in a number of ways. Note that Article 51 refers to the "inherent" right of self-defense, which has been interpreted as either pre-existing (and thereby maintained in the Charter) or as inherent in the illogic of requiring States to suffer a potentially devastating strike before acting in self-defense. Additionally, Article 2 of the Definition of Aggression resolution provides that the first use of force is merely prima facie evidence of an act of aggression. *See* Definition of Aggression, *supra* note 57, art. 2. As such, it contemplates the possibility of a first use which does not qualify as an armed attack and which, therefore, can only be justified in terms of anticipatory self-defense.

Daniel Webster following the famous *Caroline* incident. In correspondence with his British counterpart regarding an incursion into U.S. territory to attack Canadian rebels during the Mackenzie Rebellion, Webster opined that the right of self-defense applied only when "the necessity of that self-defense is instant, overwhelming, and leaving no moment for deliberation."[73] Although the incident actually had nothing to do with actions taken in anticipation of attack (the attacks in question were ongoing), Webster's formulation has survived as the classic expression of the temporal threshold for anticipatory defensive actions;[74] indeed, the Nuremberg Tribunal cited the *Caroline* case with approval.[75]

Following the events of September 11th, 2001, the United States suggested that a new self-defense paradigm was needed. As President Bush noted in his 2002 National Security Strategy:

> For centuries, international law recognized that nations need not suffer an attack before they can lawfully take action to defend themselves against forces that present an imminent danger of attack. Legal scholars and international jurists often conditioned the legitimacy of pre-emption on the existence of an imminent threat—most often a visible mobilization of armies, navies, and air forces preparing to attack.
>
> We must adapt the concept of imminent threat to the capabilities and objectives of today's adversaries. Rogue states and terrorists do not seek to attack us using conventional means. They know such attacks would fail. Instead, they rely on acts of terror and, potentially, the use of weapons of mass destruction—weapons that can be easily concealed, delivered covertly, and used without warning.[76]

His conclusion was that the "greater the threat, the greater is the risk of inaction—and the more compelling the case for taking anticipatory action to defend ourselves, even if uncertainty remains as to the time and place of the enemy's attack."[77] The United States has maintained this approach to the present.[78]

---

73. Letter from Daniel Webster, U.S. Sec'y of State, to Lord Ashburton, British Special Minister (Aug. 6, 1842), *reprinted in* 2 JOHN BASSETT MOORE, A DIGEST OF INTERNATIONAL LAW 412 (1906).

74. *See, e.g.*, THOMAS M. FRANCK, RECOURSE TO FORCE: STATE ACTION AGAINST THREATS AND ARMED ATTACKS 97 (2002).

75. *See* International Military Tribunal (Nuremberg), Judgment and Sentences, Oct. 1, 1946, *reprinted in* 41 AM. J. INT'L L. 172, 205 (1947).

76. THE WHITE HOUSE, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 15 (2002).

77. *Id.*

78. *See, e.g.*, THE WHITE HOUSE, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 18 (2006). The Obama National Security Strategy does not expressly adopt the doctrine of pre-emption, but nor is it rejected. It specifi-

Despite being characterized by some as revolutionary, even unlawful, the pre-emption doctrine represented a reasonable accommodation to the changed circumstances cited by the President. Indeed, it is arguable that the approach represented a *de minimus* departure from existing law. The underlying premise of anticipatory self-defense is that to effectively defend themselves, states must sometimes act before an aggressive blow falls. Traditionally, a standard requiring temporal proximity to the armed attack had been employed to assess the need. The underlying intent of the standard was to allow as much opportunity as possible for non-forceful measures to work in alleviating the crisis. Yet, as correctly noted in the National Security Strategy, the *modus operandi* of terrorists is to strike without warning, thereby denuding the opportunity the victim-state has to anticipatorily defend itself.

In such circumstances, the most reasonable accommodation of the law of self-defense to both the changed threat and to international law's rebuttable presumption against the legality of using force lies in restricting the victim-state from acting forcefully in self-defense until the point at which its window of opportunity to mount an effective defense is about to close. The imminency criterion should therefore not be measured by reference to the moment of armed attack, but rather with regard to the point at which a state must act defensively, lest it be too late.[79]

The "last feasible window of opportunity" standard must not be interpreted as permitting *preventive* strikes, that is, those against a prospective attacker who lacks either the means to carry out an attack or the intent to do so. The fact that an overtly hostile state is capable of launching cyber attacks—even devastating ones—does not alone entitle a potential victim to act defensively with force. Such hostility must mature into an actual decision to attack. The decision may be evidenced by, for example, preparatory cyber operations amounting to a demonstration of "hostile intent."[80] Moreover, the circumstances must be such that the pending attack has to be responded to immediately if the victim-state is to have any reasonable hope of fending it off. Consider a state's introduction of cyber vulnerabilities into another state's critical infrastructure. Such an action might amount to a use of force, but the victim-state may not react forcefully until it reasonably concludes that: 1) its opponent has decided to

---

cally reserves the right to act unilaterally. *See* 2010 NATIONAL SECURITY STRATEGY, *supra* note 6, at 22.

79. For a fuller discussion, see Michael N. Schmitt, *Responding to Transnational Terrorism under the* Jus ad Bellum*: A Normative Framework*, 56 NAVAL L. REV. 1, 16-19 (2008).

80. The U.S. Standing Rules of Engagement define hostile intent as "[t]he threat of imminent use of force against the United States, US forces, or other designated persons or property. It also includes the threat of force to preclude or impede the mission and/or duties of US forces, including the recovery of US personnel or vital USG property." CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTIONS, CJCSI 3121.01B, STANDING RULES OF ENGAGEMENT/STANDING RULES FOR THE USE OF FORCE FOR U.S. FORCES, at A-4(2005).

actually exploit those vulnerabilities; 2) the strike is likely to generate consequences at the armed attack level; and 3) it must act immediately to defend itself. Until arriving at these conclusions, the victim-state's response would be limited to non-forceful measures, including countermeasures, and referral of the matter to the Security Council.

Although transnational terrorism represents the obvious justification for the approach, cyber operations present many of the same challenges to application of the traditional temporal criterion. Like terrorism, cyber operations are typically launched without any warning that attack is imminent. The time between launch of an operation and impact is measured in seconds at most, thereby often depriving the victim of an opportunity to foil the initial attack as it is unfolding; viable defenses could resultantly be limited to passive measures, such as firewalls and antivirus software. Moreover, although the immediate severity of a cyber armed attack may not reach the level of attacks with weapons of mass destruction, cyber operations have the potential, because of networking, to affect many more individuals and activities. In light of these realities, an approach centering on a state's opportunity to defend itself is no less suitable in the context of cyber operations than in that of terrorism. Cyber or kinetic operations designed to foil an attack which has been approved, and which qualifies as an armed attack, would therefore be lawful when it reasonably appears that failure to act promptly will deprive the target State of any viable opportunity to defend itself.

C. *Criteria for Engaging in Self-Defense*

Actions in self-defense must meet two legal criteria—necessity and proportionality. The ICJ acknowledged both in the *Nicaragua* case, and later confirmed them in its *Oil Platforms* judgement.[81] Necessity requires that there be no reasonable option other than force to effectively deter an imminent attack or defeat one that is underway. This does not mean that force need represent the only available response; it merely requires that defense necessitate actions that are forceful in nature as a component of an overall response, which may well also include non-forceful measures such as diplomacy, economic sanctions, or law enforcement measures.

Proportionality, by contrast, addresses the issue of how much force is permissible once it is deemed necessary. The criterion limits the scale, scope, duration, and intensity of the defensive response to that which is required to neutralize a prospective attack or repel one that is underway. It does not restrict the amount of force used to that employed in the armed attack, since more force may be needed to successfully conduct a defense; of course, less may suffice. In addition, there is no requirement that the defensive force be of the same nature as that constituting the armed attack. Cyber operations may be responded to with kinetic opera-

81. *See Oil Platforms* (Iran v. U.S.), 2003 I.C.J. 161, 183, 196-98 (Nov. 6); *Nicaragua* (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 194 (June 27).

tions and vice versa. The point of reference is the need to effectively defend oneself, not the character of the armed attack.

The key to the necessity analysis in the cyber context is the existence, or lack thereof, of alternative, non-forceful courses of action. Should passive cyber defenses be adequate to thwart a cyber armed attack, forceful defensive measures would be disallowed. Similarly, if active cyber operations not rising to the level of force are adequate to deter armed attacks (prospective or ongoing), forceful alternatives, whether cyber or kinetic, would be barred. However, when non-forceful measures alone cannot reasonably be expected to defeat an armed attack and prevent subsequent ones, destructive cyber and kinetic operations are permissible under the law of self-defense.

Any forceful defensive cyber or kinetic operations must equally be proportionate. The victim of a cyber armed attack does not have carte blanche to conduct its cyber or kinetic defense. Rather, the extent and nature of its response are limited to ensuring the victim-state is no longer subject to attack. The requirement should not be overstated. It may be that the source of the cyber armed attack is relatively invulnerable to cyber operations. This would not preclude kinetic or cyber defensive operations against other targets in an effort to compel the attacker to desist, although they must be scaled to that purpose.

D. *Evidentiary Issues*

Identification of an "attacker" poses particular problems in the cyber context. For instance, it is possible to "spoof" the origin of attack; the lone indication of where an attack originated from, or who launched it, may be an IP address or other machine discernable data. And the speed by which cyber operations proceed dramatically compresses the time available to make such determinations. How certain must the target state be as to the identity of its attacker before responding in self-defense?

Although international law sets no specific evidentiary standard for drawing conclusions as to the originator of an armed attack, a potentially useful formula was contained in the U.S. notification to the Security Council that it was acting in self-defense when it launched its October 2001 attacks against the Taliban and al-Qaeda in Afghanistan. There, U.S. Ambassador Negroponte stated that "my Government has obtained clear and compelling information that the Al-Qaeda organization, which is supported by the Taliban regime in Afghanistan, had a central role in the attacks."[82] NATO Secretary General Lord Robertson used the same language when announcing that the attacks of 9/11 fell within the ambit of

82. Permanent Rep. of the United States of America to the U.N., Letter dated 7 October 2001 from the Permanent Rep. of the United States of America to the United Nations Addressed to the President of the Security Council, U.N. Doc. S/2001/946 (Oct. 7, 2001) [hereinafter U.S. Rep. Letter].

the collective defense provisions of Article V of the North Atlantic Treaty.[83]

"Clear and compelling" is a threshold higher than the preponderance of the evidence (more likely than not) standard used in certain civil and administrative proceedings and lower than criminal law's "beyond a reasonable doubt." In essence, it obliges a state to act reasonably, that is, in a fashion consistent with the normal state practice in same or similar circumstances. Reasonable states neither respond precipitously on the basis of sketchy indications of who has attacked them nor sit back passively until they have gathered unassailable evidence. So long as the victim-state has taken reasonable steps to identify the perpetrator of an armed attack, cyber or kinetic, and has drawn reasonable conclusions based on the results of those efforts, it may respond forcefully in self-defense. That the state in fact drew the wrong conclusion is of no direct relevance to the question of whether it acted lawfully in self-defense.[84] Its responses are assessed as of the time it took action, not ex post facto.

Although the temporal aspect cannot be ignored, the time available to make the determination is merely one factor bearing on the reasonableness of any conclusion. In particular, automatic "hack-back" systems that might involve a response amounting to a use of force are neither necessarily lawful nor unlawful. Their use must be judged in light of many factors, such as the reliability of the determination of origin, the damage caused by the attack, and the range of available response options.

An analogous standard of reasonableness would apply in the case of anticipatory self-defense against an imminent cyber attack. International law does not require either certainty or absolute precision in anticipating another state's (or non-state actor's) future actions. Rather, it requires reasonableness in concluding that a potential attacker has decided to attack and wields the capability to carry out said attack, and that it must act defensively in anticipation of the attack lest it lose the opportunity to effectively defend itself. States could not possibly countenance a higher threshold, for such a standard would deprive them of a meaningful right of self-defense.

Admittedly, ascertaining a possible adversary's intentions in the cyber environment is likely to be demanding. Aside from the difficulties of accurately pinpointing identity discussed above, it will be challenging in the context of anticipatory self-defense to identify the purpose behind a particular cyber operation. For instance, is a cyber probe of a state's air de-

83. *See* NATO Sec'y Gen. Lord Robertson, Statement at NATO Headquarters (Oct. 2, 2001), *available at* http://www.nato.int/docu/speech/2001/s011002a.htm.

84. Note by way of analogy to international criminal law, that pursuant to the Statute of the International Criminal Court, a mistake of fact is grounds for excluding criminal responsibility when the mistake negates the mental element required by the crime. *See* Rome Statute of the International Criminal Court, art. 32(1), July 17, 1998, 2187 U.N.T.S. 90, 108.

fense designed merely to gather intelligence or instead to locate vulnerabilities in anticipation of an attack which is about to be launched? Obviously, such determinations must be made contextually, considering factors such as the importance of the matter in contention, degree of political tensions, statements by military and political leaders, military activities like deployments, exercises and mobilizations, failed efforts to resolve a contentious situation diplomatically, and so forth. The speed with which the defender may have to make such an assessment to effectively defend itself further complicates matters. Despite the factual and practical complexity, the legal standard is clear; a state acting anticipatorily in self-defense must do so reasonably. In other words, states in the same or similar circumstances would react defensively.

When a state asserts that it is acting in self-defense, it bears the burden of proof. In the *Oil Platforms* case, the ICJ noted that the United States had failed to present evidence sufficient to "justify its using force in self-defense"[85] Specifically, it could not demonstrate that Iran was responsible for a 1987 missile attack against an oil tanker sailing under U.S. flag or the 1988 mining of a U.S. warship during the Iran-Iraq "tanker war," to which the United States responded by attacking Iranian oil platforms. The court rejected evidence offered by the United States which was merely "suggestive," looking instead for "direct evidence" or, reframed, "conclusive evidence."[86] "Clear and compelling" evidence would meet these requirements. Thus, states responding to a cyber armed attack must be prepared to present evidence of this quality as to the source and nature of an impending attack, while those acting in anticipation of an attack must do likewise with regard to the potential attacker's intent and capability.

E. *Collective Responses*

Unlike countermeasures, defensive actions may be collective. This possibility is explicitly provided for in Article 51's reference to "individual or collective self-defense." Collective self-defense may be mounted together by states which have all been attacked or individually by a state (or states) which has not, but comes to the defense of another. Although the basic norm is clear in theory, it is complex in application. As noted in the Group of Experts' Report on the new NATO Strategic Concept, "there may well be doubts about whether an unconventional danger—such as a cyber attack or evidence that terrorists are planning a strike—triggers the collective defence mechanisms of Article 5 [the North Atlantic Treaty implementation of Article 51]."[87]

The mere fact of an armed attack allows for collective defensive action; no authorization from the Security Council is necessary. But there are legal limits on the exercise of the right. In the *Nicaragua* case, the ICJ

85. *Oil Platforms* (Iran v. U.S.), 2003 I.C.J. at 189.

86. *Id.* at 189-90, 194.

87. *NATO 2020, supra* note 7, at 20.

suggested that only the victim-state is empowered to determine whether an armed attack has occurred, and it must request assistance before others act on its behalf.[88] Absent such a determination and request, collective actions would themselves amount to unlawful uses of force, and, depending on their nature, even armed attacks (paradoxically, against the state launching the initial armed attack). These requirements are designed to prevent states from claiming to act in collective self-defense as a subterfuge for aggression.

Given the practical difficulties of identifying a cyber operation's originator, this is a sensible limitation. It must be noted that some distinguished commentators challenge the strict application of these requirements. They argue that in cases where the collective self-defense actions occur outside the territory of the victim-state, other states may be entitled to act on the basis of their own right to ensure their security. The right arguably derives from a breach of the duty to refrain from armed attack that the state initiating the armed attack bears.[89] This latter scenario is particularly germane in the cyber context since the effects of cyber armed attacks could easily spread through networks, thereby endangering states other than those which are the intended target. The prevailing view is nevertheless that there must be a request from the victim-state before the right of collective self-defense matures.

In many cases, a pre-existing treaty contemplates collective self-defense. Article 52(1) of the UN Charter provides that "nothing in the present Charter precludes the existence of regional arrangements or agencies for dealing with such matters relating to the maintenance of international peace and security as are appropriate for regional action . . . ." Despite the reference to "regional" arrangements, the agreements need not be limited to states in a particular region or to actions occurring in a defined area. Such arrangements may take multiple forms. For instance, bilateral and multilateral mutual assistance treaties typically provide that the Parties will treat an armed attack against one of them as an armed attack against all.[90] As a practical matter, the effectiveness of collective self-defense provisions usually depends on the willingness of the treaty partners to come to each other's aid. A state that does not see collective self-defensive action as in

88. *See Nicaragua* (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 199 (June 27). The Court reiterated this position in the *Oil Platforms* case of 2003. *See Oil Platforms* (Iran v. U.S.), 2003 I.C.J. at 188.

89. *See* DINSTEIN, *supra* note 69, at 270. This was the position adopted in Judge Jenning's dissent in *Nicaragua*. *See Nicaragua* (Nicar. v. U.S.), 1986 I.C.J. at 544-46 (dissenting opinion of Judge Sir Robert Jennings).

90. For instance, the Japan-United States mutual defense treaty provides that "[e]ach Party recognizes that an armed attack against either Party in the territories under the administration of Japan would be dangerous to its own peace and safety and declares that it would act to meet the common danger in accordance with its constitutional provisions and processes." Treaty of Mutual Cooperation and Security Between Japan and the United States of America, U.S.-Japan, art. V, Jan. 19, 1960, 11 U.S.T. 1632.

its national interest may be expected to contest characterization of a cyber operation as an armed attack.

Military alliances based on the right to engage in collective self-defense also exist, the paradigmatic example being the North Atlantic Treaty Organization (NATO). Pursuant to Article V of the treaty, Member States

> agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the [Member State] or [Member States] so attacked by taking forthwith, individually and in concert with the other [Member States], such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.[91]

The benefit of alliances is that they generally involve a degree of advanced planning for combined operations in the event of armed attack, and, as with NATO, military structures are often set up to coordinate and direct military operations. Preplanning and the existence of collective mechanisms for managing joint and combined action are especially valuable with regard to defending against cyber attacks. However, like mutual assistance treaties, alliance arrangements are subject to the reality that they are composed of states, which can be expected to act pursuant to their own national interests. In the case of NATO, for instance, decisions to act are taken by consensus in the North Atlantic Council; a single Member State can therefore block NATO collective action. Indeed, had the cyber operations against Estonia risen to the level of an armed attack, it is not altogether certain that NATO would have come to its defense militarily, especially in light of Russia's place in the European security environment and the countervailing commitments of NATO allies elsewhere, especially Afghanistan and Iraq.

F. *State Sponsorship of Attacks by Non-State Actors*

The issue of state sponsorship of cyber operations was addressed earlier in the context of the responsibility of states for uses of force by non-state actors. There the question was, When does a state violate the use of force prohibition by virtue of its relationship with others who conduct cyber operations? However, the issue of state sponsorship in the self-defense context is much more momentous. It asks when may forceful defensive actions, even kinetic ones, be taken against a state which has not engaged in cyber operations, but which has "sponsored" them? In other

91. North Atlantic Treaty, art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243, 246.

words, when is an armed attack attributable to a state such that the state may be treated as if it had itself launched the attack?

Until the transnational attacks of September 11, 2001, the generally accepted standard was set forth in the *Nicaragua* case. There the ICJ stated that

> an armed attack must be understood as including not merely action by regular forces across an international border, but also "the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to" (inter alia) an actual armed attack conducted by regular forces, "or its substantial involvement therein."[92]

The court noted that the activities involved should be of a "scale and effects" that would equate to an armed attack if carried out by the state's military. Thus, "acts by armed bands where such attacks occur on a significant scale" would qualify, but "a mere frontier incident would not."[93]

By this standard, attribution requires (1) acts qualifying as an armed attack and (2) that the state dispatched the non-state actors or was substantially involved in the operations. As noted earlier, the ICTY took a more relaxed view of the degree of control necessary, accepting "overall control" as sufficient.[94] The events of 9/11 brought the issue of threshold to light in a dramatic way. Assistance provided by the Taliban to al-Qaeda met neither the *Nicaragua* nor *Tadic* standards, since the Taliban merely provided sanctuary to al-Qaeda. The cyber analogy would be doing nothing to put an end to the activities of cyber "terrorists" or other malicious hackers operating from a state's territory when it is within its capability, legal and practical, to do so.

Even though there was seemingly no legal basis for attribution to Afghanistan, when the Coalition responded with armed force against both al-Qaeda and the governing Taliban, no objection was raised. On the contrary, the Security Council condemned the Taliban "for allowing Afghanistan to be used as a base for the export of terrorism by the Al-Qaida network and other terrorist groups and for providing safe haven to Usama Bin laden, Al-Qaida and others associated with them."[95] It seems that the international community had lowered the normative bar of attribution measurably. While the underlying operations must still amount to an armed attack, it is arguable that today much less support is required for attribution than envisaged in either *Nicaragua* or *Tadic*. Far from being counter-legal, this process of reinterpretation is natural; understandings of

92. *Nicaragua* (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 195 (citation omitted).

93. *Id.*

94. It must be emphasized that the legal issue involved in that case was not attribution of an armed attack, but rather the existence of an international armed conflict.

95. S.C. Res. 1378, pmbl., U.N. Doc. S/RES/1378 (Nov. 14, 2001).

international legal norms inevitably evolve in response to new threats to the global order. In that cyber operations resemble terrorism in many regards, states may equally be willing to countenance attribution of a cyber armed attack to a state which willingly provides sanctuary to non-state actors conducting them.

G. *Armed Attacks by Non-State Actors*

Although most cyber operations are launched by individuals such as the anti-Estonian "hacktivists," concern is mounting about the prospect that transnational terrorist organizations and other non-state groups will turn to cyber operations as a means of attacking states.[96] The concern is well-founded. Al-Qaeda computers have been seized that contain hacker tools, the membership of such groups is increasingly computer-literate, and the technology to conduct cyber operations is readily available. In one case, a seized al-Qaeda computer contained models of dams, a lucrative cyber attack target, and the computer programs required to analyze them.[97]

International lawyers have traditionally, albeit not universally, characterized Article 51 and the customary law of self-defense as applicable solely to armed attacks mounted by one state against another. Violent actions by non-state actors fell within the criminal law paradigm. Nonetheless, the international community treated the 9/11 attacks by al-Qaeda as armed attacks under the law of self-defense. The Security Council adopted numerous resolutions recognizing the applicability of the right of self-defense.[98] International organizations such as NATO and many individual states took the same approach.[99] The United States claimed the right to act forcefully in self-defense,[100] and no state objected to the assertion. Lest this approach be dismissed as simply an emotive reaction to the horrific attacks of 9/11, it must be noted that when Israel launched operations into Lebanon in response to Hezbollah's 2006 terrorism, the

96. *See* 2010 NATIONAL SECURITY STRATEGY, *supra* note 6, at 27; *NATO 2020*, *supra* note 7, at 17.

97. *See* CLAY WILSON, CONG. RESEARCH SERV., RL32114, COMPUTER ATTACK AND CYBER TERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS, 11-13 (2003).

98. *See, e.g.*, S.C. Res. 1373, U.N. DOC. S/RES/1373 (Sept. 28, 2001); S.C. Res 1368, U.N. DOC. S/RES/1368 (Sept. 11, 2001).

99. *See, e.g.*, Org. of American States, *Terrorist Threat to the Americas*, OAS DOC. RC.24/RES.1/01 (Sept. 21, 2001); Brendan Pearson, *PM Commits to Mutual Defence*, AUSTRALIAN FIN. REV., Sept. 15, 2001, at 9; Press Release, NATO, Statement by the North Atlantic Council (Sept. 12, 2001), *available at* http://www.nato.int/docu/pr/2001/p01-124e.htm.

100. "In response to these attacks, and in accordance with the inherent right of individual and collective self-defence, United States armed forces have initiated actions designed to prevent and deter further attacks on the United States. These actions include measures against Al-Qaeda terrorist training camps and military installations of the Taliban regime in Afghanistan." U.S. Rep. Letter, *supra* note 82.

international community again seemed to accept a country's right to defend itself against armed attacks mounted by non-state actors.[101]

Despite acceptance by states of the premise that non-state actors may qualify as the originators of an armed attack, the ICJ seems to have taken a step backwards in two post-9/11 cases. In the advisory opinion on the *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*[102] and the *Armed Activities on the Territory of the Congo*[103]case, the ICJ refrained from considering claims of self-defense against actions by non-state actors, noting that no assertion had been made that the relevant actions were imputable to a state.[104] Although the court's reasoning was nuanced and fact-specific, it has nevertheless been widely criticized as inattentive to contemporary understandings of the relevant law. In particular, in the *Wall* case, three judges expressly departed from the majority's approach on the bases that it ignored the fact that Article 51 makes no mention of the originator of an attack (while Article 2(4) specifically addresses uses of force by states) and that the Security Council had deliberately treated terrorist attacks as armed attacks in the aftermath of the 9/11.[105]

The court's hesitancy to embrace the notion of armed attack by non-state actors is understandable in light of the risk of abuse. States might well apply it to engage in robust military operations against groups in situations in which law enforcement is the more normatively appropriate response. For instance, significant concerns have been raised regarding counterterrorist operations occurring outside an armed conflict mounted in states which do not consent to them. Such concerns are likely to be even more acute in relation to cyber operations, which are conducted not by armed members of groups resembling classic military forces, but rather by cyber experts equipped with computers. Nevertheless, as a matter of law, states seem comfortable with applying the concept of armed attacks to situations involving non-state actors. Should such groups launch cyber attacks meeting the threshold criteria for an armed attack, states would likely respond within the framework of the law of self-defense.

The point that the attacks must meet the threshold criteria cannot be overemphasized. There is no state practice supporting extension of the concept to the actions of isolated individuals, such as hacktivists or patri-

101. *See generally* Michael N. Schmitt, *"Change Direction" 2006: Israeli Operations in Lebanon and the International Law of Self-Defense*, 29 MICH. J. INT'L L. 127 (2008). Many commentators and States saw the actions as violating the proportionality criterion discussed above.

102. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (*Wall*), Advisory Opinion, 2004 I.C.J. 136 (July 9).

103. Armed Activities on the Territory of the Congo (*Congo*) (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, ¶ 160 (Dec. 19).

104. *See Congo* (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, 217 (Dec. 19); *Wall*, Advisory Opinion, 2004 I.C.J. 136, ¶ 139 (July 9).

105. *See Wall*, 2004 I.C.J. 136, ¶ 6 (separate declaration of Judge Buergenthal); *id.* ¶ 33 (separate opinion of Judge Higgins); *id.* ¶ 35 (separate opinion of Judge Koojmans).

otic hackers. Further, the cyber operations must be severe enough to qualify as armed attacks, that is, they have to result in damage to or destruction of property or injury to or death of individuals. Finally, as the debate over minor border incursions demonstrates, it is uncertain whether attacks which meet the aforementioned threshold, but are not of significant scale, would qualify. As an example, a cyber attack that caused a single plant's generator to overheat, thereby temporarily interrupting service until it could be repaired, would presumably not, by the more restrictive standard, qualify as an armed attack. Rather, it would be the cyber equivalent of a border incursion.

H. *Cross-Border Operations*

When armed attacks by non-state actors emanate from outside a state, may that state take defensive actions against its perpetrators in the territory of the state where they are based? This question has been raised recently in the context of unmanned aerial vehicle strikes against terrorists in Pakistan and elsewhere. It is no less pertinent to situations involving cyber armed attacks launched by non-state actors from abroad.

It is indisputable that one state may employ force in another with the consent of the territorial state. For instance, a state may grant others the right to enter its territory to conduct counterterrorist operations, as often occurs in Pakistan, or a state embroiled in an internal conflict with insurgents may request external assistance in restoring order, as with International Security Assistance Force (ISAF) operations in Afghanistan or United States Forces (USF) in Iraq. A State subjected to an armed attack, whether cyber or kinetic, could, with the acquiescence of the territorial state, equally launch cyber defensive operations into the state from which the attacks emanated.

The legal dilemma arises when operations are conducted without territorial state approval. By the principle of sovereignty (and the derivative notion of territorial integrity), a state enjoys near absolute control over access to its territory. In affirmation, the UN General Assembly has cited the use of force by a state on the territory of another as an act of aggression.[106] Yet, the right of states to use force in self-defense is no less foundational. When terrorists or insurgents seek sanctuary in a state other than that in which they are conducting operations, they bring the territorial state's right of sovereignty into conflict with the victim-state's right of self-defense.

Fortunately, international law does not require an either-or resolution when norms clash. Instead, it seeks to balance them by fashioning a compromise which best achieves their respective underlying purposes. In this case, such a balance would ensure that the territorial state need not suffer unconstrained violations of its sovereignty, but nor would the victim-state have to remain passive as non-state groups attack it with impunity from

106. *See* Definition of Aggression, *supra* note 57, art. 3(a).

abroad. The resulting compromise is as follows. The victim-state must first demand the territorial state fulfill its legal duty to ensure actions on or from its territory do not harm other states and afford the territorial state an opportunity to comply.[107] If that state subsequently takes effective steps to remove the threat, then penetration of its territory by the victim-state, whether kinetically or by cyber means, is impermissible. But if the territorial state fails to take appropriate and timely action, either because it lacks the capability to conduct the operations or simply chooses not to do so (e.g., out of sympathy for the non-state actors or because its domestic laws preclude action), the victim-state may act in self-defense to put an end to the non-state actor's attacks. It matters not whether the actions are kinetic or cyber in nature, as long as they comply with the principles of proportionality and necessity.

V. FAULT LINES IN THE LAW

The legal analysis set forth above should strike most readers as unsatisfactory. Clear fault lines in the law governing the use of force have appeared because it is a body of law that predates the advent of cyber operations. The normative scheme made sense when close congruity existed between the coercive instruments of international relations, particularly military force, and their effects. To the extent one state disrupted order in the international community, it usually did so by using force to harm objects and persons. Resultantly, instrument-based normative shorthand (use of *force, armed* attack, and *armed* conflict) was employed as a means of precluding those effects (death, injury, destruction, and damage) which were perceived as most disruptive of community stability, and as most threatening to state security. Debates such as whether actions short of military operations are uses of force or whether minor border incursions qualify as armed attacks demonstrate that the foundational concerns were actually consequence-based, for both reflect recognition that the instrument-based approach is not perfectly calibrated.

The advent of cyber operations threw the instrument-based approach into disarray by creating the possibility of dramatically destabilizing effects caused by something other than kinetic actions. They weakened the natural congruency between the normative shorthand employed in the law governing resort to force and those consequences which the law sought to avoid as disruptive. Conceptually, the qualitative scheme, by which prohibitions were expressed in terms of types of activities (use of the military and other destructive instruments as distinguished from non-destructive ones), no longer sufficed to preclude those effects about which states had become most concerned. A non-kinetic, non-destructive means of generating effects which states cannot possibly countenance now existed;

107. On the duty to police one's own territory, see Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4 (Apr. 9).

the qualitative shorthand no longer tracked the quantitative concerns of states.

The prohibition on the use of force has proven somewhat adaptable to this new reality because it has long been understood to extend beyond the application of kinetic force. Thus, it is reasonable to employ the criteria suggested in this Article to identify situations in which non-kinetic actions will result in quantitatively unacceptable, and therefore prohibited, consequences. The UN Charter mechanism for Security Council-based responses to threats to the peace, breaches of the peace, and acts of aggression is likewise adaptable because by it threats to the peace include, simply put, whatever the Council wishes.

Evidence of disquiet abounds. In a recent report by the National Academy of Science, examples of armed attack included "cyberattacks on the controlling information technology for a nation's infrastructure that had a significant impact on the functioning of that infrastructure (whether or not it caused immediate large-scale death or destruction of property)" and "a cyberattack against the stock exchanges that occurs repeatedly and continuously, so that trading is disrupted for an extended period of time (e.g., days or weeks)."[108] As a matter of law, they would likely qualify as uses of force, but not, by a strict interpretation of the self-defense norm, as armed attacks (or as initiating an armed conflict). The problem is that most states would surely treat them as such. In other words, the National Academy report has misconstrued the law, but accurately identified probable state behavior.

When state expectations as to the "rules of the game" deviate from those that actually govern their actions, new norms can emerge. One method by which this can occur is through new treaty law. However, it is highly unlikely that any meaningful treaty will be negotiated to govern cyber operations in the foreseeable future. The greatest obstacle is that those states which are most vulnerable to cyber operations tend to be those which are also most capable of conducting them. Such tension will cause such states to hesitate before agreeing to prohibitions designed to protect them which may also definitively limit their freedom of action. This is especially so in light of the nascent nature of cyber warfare and the lack of experience of most states in these operations. In international relations, states are often comfortable with a degree of vagueness.

Much more likely is the emergence of new understandings of the existing treaty law which are responsive to the realities of cyber operations. While only subsequent treaty action can technically alter a treaty's terms, state practice can inform their interpretation over time. A well-known example involves veto action by permanent members of the Security Council. The UN Charter provides that a binding resolution of the Council requires the affirmative vote of all five permanent members.[109] However,

108. NAT'L RESEARCH COUNCIL, *supra* note 70, at 254-55.

109. *See* U.N. Charter art. 27(3).

state practice has been to treat the provision as blocking action only when a member of the "P5" vetoes a proposed resolution. This counter-textual interpretation is now accepted as the law.[110] The recent extension of the notion of armed attack to actions by non-state actors similarly illustrates normative evolution prompted by shifting state expectations.

In due course, similar evolution in how the concept of armed attack is understood should be anticipated, as states increasingly accept the proposition that armed attacks must be judged qualitatively *and* quantitatively. Consequences will remain the focus of concern, but they will be assessed both in terms of their nature and as to their impact on affected states. In this regard, the seven criteria proffered above in the use of force context can serve as useful indicators of whether states are likely to characterize particular cyber operations as armed attacks (or as initiating an armed conflict), and thus suggest the probable vector of the law. However, for the moment the existing law remains intact; it will be left to states to articulate the expectations and engage in practices that can serve to fuel the normative process necessary to transform *lex ferenda* into *lex lata*.[111]

---

110. *See* Bruno Simma, Stefan Brunner & Hans-Peter Kaul, *Article 27, in* 1 THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 476, 493-98 (Bruno Simma ed., 2d ed. 2002). The veto principle does not apply to votes on procedural matters.

111. The law as it should be and the law that is, respectively.