2011

Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)

Matthew C. Waxman
Columbia Law School, mwaxma@law.columbia.edu

Article

Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)

Matthew C. Waxman[†]

I. INTRODUCTION

Suppose that the United States, in opposing Iran's suspected development of nuclear weapons, decides that the best way to halt or slow Iran's program is to undermine the Iranian banking system, calculating that the ensuing financial pressure would dissuade or prevent Iran from continuing on its current course. And further suppose that the United States draws up the following four options, all of which are believed likely to produce roughly the same impact on Iran's financial system and have similar effects on Iran's economy and population:

(1) Military air strikes against key Iranian banking facilities to destroy some of the financial system's physical infrastructure;

---

† Associate Professor, Columbia Law School; Adjunct Senior Fellow, Council on Foreign Relations; Member of the Hoover Institution Task Force on National Security and Law. I thank the following for their comments on earlier drafts of this paper: Gabriella Blum, Philip Bobbitt, Jeffrey Cooper, Ashley Deeks, Joshua Dorosin, Colleen Garcia, Jack Goldsmith, Duncan Hollis, Eric Jensen, Sean Kanuck, David Kaye, Andrew McLaughlin, Saira Mohamed, Daniel Prieto, Adam Segal, Bo Simmons, Paul Stephan, Tim Wu, and workshop participants at Columbia Law School and the Hoover Institution Task Force on National Security and Law.

(2) A regulatory cut-off of Iranian banks from the U.S. financial system, making it difficult for Iran to conduct dollarized transactions;[1]
(3) Covert flooding of the Iranian economy with counterfeit currency and other financial instruments;
(4) Scrambling Iranian banking data by infiltrating and corrupting its financial sector's computer networks.

Which of these options constitute uses of force, subject to the U.N. Charter's prohibitions and self-defense provisions?

I pose this set of hypothetical options for several reasons. First, it is an exercise in legal line drawing. The development and deployment of new technologies—both their offensive potential and the vulnerabilities they create for states reliant on those technologies—raise questions about permissible versus impermissible modes of interstate conduct and conflict. Military attacks are generally illegal, with exceptions for self-defense or when authorized by the U.N. Security Council.[2] Most economic and diplomatic measures, even if they exact tremendous costs on target states (including significant loss of life), are generally not barred by the U.N. Charter, though some of them may be barred by other legal principles.[3] Where along the spectrum of permissible to impermissible conduct do various types of cyber-attacks lie?

Definitions of cyber-attacks vary, and the range of hostile activities that can be carried out over information networks is immense, ranging from malicious hacking and defacement of websites to large-scale destruction of the military or civilian infrastructures that rely on those networks. By "cyber-attacks" I mean efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them,[4] which is still a broad category. That breadth—encompassing activities that range in target (military versus civilian, public versus private), consequences (minor versus major, direct versus indirect), and duration (temporary versus long-term)—is part of what makes international legal interpretation or regulation in this area so difficult.

Global interconnectedness brought about through linked digital information networks brings immense benefits, but it also places a new set of offensive weapons in the hands of states and nonstate actors, including terrorist groups.[5] Military defense networks can be remotely disabled or damaged.[6]

---

1. For a discussion of this capability, see Juan C. Zarate, *Harnessing the Financial Furies: Smart Financial Power and National Security*, WASH. Q., Oct. 2009, at 43.

2. *See infra* notes 19-31 and accompanying text.

3. *See infra* notes 32-36 and accompanying text.

4. This definition is based heavily on the one used in COMM. ON OFFENSIVE INFO. WARFARE, NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 10-11 (2009) [hereinafter NRC COMMITTEE REPORT].

5. Estimates vary widely about the threat of cyber-attacks and cyber-war. Former Director of National Intelligence Michael McConnell argues that "[t]he United States is fighting a cyber-war today, and we are losing. . . . As the most wired nation on Earth, we offer the most targets of significance, yet our cyber-defenses are woefully lacking." Mike McConnell, *To Win the Cyber-War, Look to the Cold War*, WASH. POST, Feb. 28, 2010, at B1. Others experts believe that cyber-espionage—stealing government and corporate secrets through infiltration of information systems—is a major challenge, but

Private sector networks can be infiltrated, disrupted, or destroyed.[7] "Denial of service" attacks—flooding an Internet site, server, or router with data requests to overwhelm its capacity to function—can be used to take down major information networks. This method of attack was demonstrated in Estonia (one of the most "wired" nations in the world) during a period of diplomatic tensions with Russia in 2007,[8] when such attacks disrupted government and commercial functions for weeks, including banking, media, and communications.[9] More recently, it has been widely reported that a computer code dubbed Stuxnet, perhaps created and deployed by the United States or Israel, infected and significantly impaired Iran's uranium enrichment program by disrupting parts of its control system.[10]

The London-based International Institute for Strategic Studies recently highlighted "the growing consensus" that future conflicts may feature "the use of cyber-warfare to disable a country's infrastructure, meddle with the integrity of another country's internal military data, try to confuse its financial transactions or to accomplish any number of other possibly crippling aims."[11] A

---

that threat assessments of major cyber-attacks are overblown. *See* Seymour M. Hersh, *The Online Threat*, NEW YORKER, Nov. 1, 2010, at 44, 48.

Many experts assess that terrorist or criminal groups pose cyber-threats, too, but that for now the greatest potential for damage through cyber-attacks lies with a handful of states. *See* CTR. FOR STRATEGIC & INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 13 (2008), *available at* http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf ("Our most dangerous opponents are the militaries and intelligence services of other nations. They are sophisticated, well resourced, and persistent. Their intentions are clear, and their successes are notable."); Bill Gertz, *China Bolsters for "Cyber Arms Race" with U.S.*, WASH. TIMES, May 12, 2009, at A1 (discussing Russia and China as the main peers to the United States in cyber-warfare capability). This is not to deny that terrorist or criminal groups also pose a significant threat. *See* William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, FOREIGN AFF., Sept./Oct. 2010, at 97, 101. Thus far, however, terrorist groups have focused their cyber-activities on propaganda. *See War in the Fifth Domain: Are the Mouse and Keyboard the New Weapons of Conflict?*, ECONOMIST, July 1, 2010, at 25, 27. The possibility that terrorist groups or other nonstate or private actors might resort to cyber-attacks would also raise questions of state attribution. For example, questions arise as to whether actions by nonstate actors may legally be imputed to a state that allowed the cyber-attacks to occur in its territory or supported the attackers in other ways. The fact that a state may use a third-party state's territory, infrastructure, or information systems as part of an offensive or defensive cyber-operation also implicates a host of self-defense issues and questions under neutrality law. For a discussion of these issues, see Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 232-39 (2002); *see also infra* note 171 (noting issues involved with attempting to attribute nonstate actors' attacks to state supporters).

6. *See* Lynn, *supra* note 5, at 97.

7. For a discussion of offensive cyber-attack capabilities and scenarios, see *id.* at 100-01.

8. *See* Evgeny Morozov, *The Fog of Cyberwar*, NEWSWEEK (Apr. 18, 2009), http://www.newsweek.com/2009/04/17/the-fog-of-cyberwar.html; John Schwartz, *When Computers Attack*, N.Y. TIMES, June 24, 2007, at 1; Ian Traynor, *Russia Accused of Unleashing Cyberwar To Disable Estonia*, GUARDIAN, May 17, 2007, at 1.

9. *See* Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 193-94 (2009). According to the Estonian Defense Minister, "All major commercial banks, telcos, media outlets, and name servers—the phone books of the Internet—felt the impact, and this affected the majority of the Estonian population. This was the first time that a botnet threatened the national security of an entire nation." Joshua Davis, *Web War One*, WIRED, Sept. 2007, at 165, 165 (quoting the Estonian Defense Minister).

10. *See* Ken Dilanian, *Iran and the Era of Cyber War*, L.A. TIMES, Jan. 17, 2011, at A1; David E. Sanger, *Iran Fights Malware Attacking Computers*, N.Y. TIMES, Sept. 26, 2010, at 4.

11. Press Release, John Chipman, Dir.-Gen. & Chief Exec., Int'l Inst. for Strategic Studies, Military Balance 2010—Press Statement (Feb. 3, 2010), *available at* http://www.iiss.org/publications/military-balance/the-military-balance-2010/military-balance-2010-press-statement/.

U.N.-convened panel of governmental experts recently echoed that conclusion, noting that "existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century. . . . Their effects carry significant risk for public safety, the security of nations and the stability of the globally linked international community as a whole."[12] In short, electronic and informational interconnectivity creates tremendous vulnerabilities, and some experts speculate that the United States may be especially at risk because of its high economic and military dependency on networked information technology.[13]

Computer information system capabilities and vulnerabilities raise international legal questions of tremendous public policy import. What are the permissible uses of offensive cyber-capabilities? To what extent is existing international law adequate to regulate these capabilities today and in the future? And what international legal authority do states have to respond, including with military force, to cyber-attacks or cyber-threats by states or nonstate actors? Note that I am concerned here with *jus ad bellum* issues—including whether cyber-attacks constitute an act of aggression or would justify resort to armed force in response—but not *jus in bello* issues, that is, how the laws of war would govern the use of cyber-attacks during an ongoing armed conflict.[14]

Besides illustrating some new interpretive challenges with regard to the U.N. Charter, another reason I pose the opening hypothetical is to illustrate that legal line drawing with respect to cyber-attacks will produce winners and losers, and to illuminate the implications of those disparate effects for international legal development. States have different capabilities and different vulnerabilities to those capabilities. Not all states, for example, have the financial and trade muscle to coerce other states economically, and states have varying strength to withstand economic pressure. The same is true of cyber-attack and defense capabilities, so legal rules that affect the costs of using cyber-attacks have disparate strategic consequences. Legal line drawing with respect to the use of force and modes of conflict has distributive effects on power, and is therefore likely to be shaped by power relations.[15] For major

12. *See* Rep. of the Grp. of Governmental Experts on Dev. in the Field of Info. & Telecomm. in the Context of Int'l Sec., 65th Sess., ¶ 1, U.N. Doc. A/65/201 (July 30, 2010).

13. *See* NRC COMMITTEE REPORT, *supra* note 4, at 18-20; Walter Gary Sharp, Sr., *The Past, Present, and Future of Cybersecurity*, 4 J. NAT'L SECURITY L. & POL'Y 13 (2010). For a discussion of early U.S. government concerns about such vulnerabilities during the 1990s, see Charles J. Dunlap, Jr., *How We Lost the High-Tech War of 2007: A Warning from the Future*, WKLY. STANDARD, Jan. 29, 1996, at 22; and Mark Thompson & Douglas Waller, *Onward Cyber Soldiers*, TIME, Aug. 21, 1995, at 38.

14. For a discussion of *jus in bello* issues in relation to cyber-attacks, see, for example, NRC COMMITTEE REPORT, *supra* note 4, at 262-68. In many future cases, the most vexing legal questions will not involve whether a cyber-attack alone is legally prohibited or justifies self-defense, but rather whether cyber-attacks are a legal means of engaging in a conflict that has already erupted. A useful illustration is Russia's alleged cyber-attacks on Georgian public and private information networks during the 2008 conflict amid significant conventional military operations. *See* 2 REPORT OF THE INDEPENDENT INTERNATIONAL FACT-FINDING MISSION ON THE CONFLICT IN GEORGIA 217-19 (2009), *available at* http://www.ceiig.ch/pdf/IIFFMCG_Volume_II.pdf.

15. For a discussion of the distributive effects of international use of force rules, see Matthew C. Waxman, *Self-Defense and the Limits of WMD Intelligence*, *in* FUTURE CHALLENGES IN NATIONAL SECURITY AND LAW 14-15 (Peter Berkowitz ed., 2010), *available at* http://www.hoover.org/taskforces/

actors like the United States, aligning legal interpretation with strategic interests is exceptionally difficult because the future effects of information technology on power and conflict remain so uncertain.

To better understand contemporary relationships between international law regulating force and cutting-edge technologies, this Article looks backward in time to international legal disputes and scholarly debates of the Cold War. A central theme is that these fundamental issues are not entirely new or unique to cyber-technology, even if they have new dimensions that make them harder to solve or navigate. Modes and technologies of conflict change, and the law adjusts with varying degrees of success to deal with them.[16] Throughout the U.N. Charter regime's sixty-plus years of development, the means by which states and international actors wage conflict has changed so dramatically that every so often major international legal figures debate whether the Charter's most basic tenets are "dead."[17] Cyber-warfare capabilities and vulnerabilities will strain the Charter and its basic prohibition on force once again, and the lessons of history can help us understand how.

This Article makes two overarching arguments. First, strategy is a major driver of legal evolution. Most scholarship and commentary on cyber-attacks capture only one dimension of this point, focusing on how international law might be interpreted or amended to take account of new technologies and threats. The focus here, however, is on the dynamic interplay of law and strategy—strategy generates reappraisal and revision of law, while law itself shapes strategy—and the moves and countermoves among actors with varying interests, capabilities, and vulnerabilities. The purpose is not to come down in favor of one legal interpretation or another, and the conclusions are necessarily speculative because no governments speak in much detail about their cyber-warfare capabilities and strategies at this point. There are downside risks and tensions inherent in any plausible approach, though, and this analysis helps in understanding their implications.

Second, it will be difficult to achieve international agreement on legal interpretation and to enforce it with respect to cyber-attacks.[18] The current trajectory of U.S. interpretation is a reasonable effort to overcome the translation problems inherent in a U.N. Charter built for a different era of conflict. However, not only do certain features of cyber-activities make international legal regulation very difficult, but major actors also have divergent strategic interests that will pull their preferred doctrinal interpretations and aspirations in different directions, impeding formation of a

---

national-security/challenges.

16. *See* Yoram Dinstein, *Computer Network Attacks and Self-Defense*, 76 INT'L L. STUD. 99, 114-15 (2002) ("The novelty of a weapon—any weapon—always baffles statesmen and lawyers, many of whom are perplexed by technological innovation. . . . [A]fter a period of gestation, it usually dawns on belligerent parties that there is no insuperable difficulty in applying the general principles and rules of international law to the novel weapon . . . .").

17. *See, e.g.*, David Wippman, *The Nine Lives of Article 2(4)*, 16 MINN. J. INT'L L. 387 (2007).

18. In that regard, I am less sanguine than scholars like Anthony D'Amato, who "predict[s] that attacks on the Internet will soon be seen as clearly illegal under international law" and suggests that "customary international law [may have] already reached that position." Anthony D'Amato, *International Law, Cybernetics, and Cyberspace*, 76 INT'L L. STUD. 59, 67 (1999).

stable international consensus. U.S. policymakers should therefore prepare to operate in a highly contested and uncertain legal environment. The prescription is not to abandon interpretive or multilateral legal efforts to regulate cyber-attacks; rather, it is to recognize the likely limits of these efforts and to consider the implications of legal proposals or negotiations in the context of broader security strategy.

The Article proceeds as follows. Part II dissects a long-running debate over the meaning of "force" and "armed attack" in Articles 2(4) and 51 of the U.N. Charter, and examines the challenges of fitting cyber-attacks into existing legal categories. This Part does not offer a doctrinal conclusion about where the lines should ultimately be drawn, though it discusses the most salient merits and problems of alternative interpretations. Instead, this Part uses the hypothetical options laid out above as a way to illustrate the implications of competing interpretations, which echo past interpretive disputes. It also describes the general thrust of U.S. government doctrinal thinking about cyber-warfare and the regulation of force, which emphasizes the *effects* of cyber-attacks in analyzing whether they cross the U.N. Charter's legal thresholds.

Part III considers parallels between cyber-warfare and the "low-intensity conflict" or proxy warfare waged by the superpowers and their clients during the Cold War. As in that latter context, the low visibility of states' moves and countermoves in cyberspace will slow the process of interpretive development. This Part draws on Cold War lessons to argue that Article 2(4) will probably be a weak constraint on offensive cyber-attacks because of, among other reasons, the difficulty of observing them and attributing them to their sources or sponsors. Those weaknesses will also likely plague any attempt to negotiate and enforce new international agreements limiting cyber-warfare.

Part IV draws again on early Charter history to argue that interpretations of Articles 2(4) and 51 have distributive effects on power and therefore have strategic consequences. Rather than urging one interpretation or another, this Part aims to shed light on the strategic logic likely driving U.S. legal thinking, and it urges a more cautious and multidimensional assessment than is usually found in this burgeoning scholarly field. Whether emergent U.S. interpretations of the Charter serve U.S. interests or broader international societal goals of global order depends on the validity of assumptions about an unpredictable future security environment.

II. ARTICLE 2(4) AND THE MEANING OF "FORCE"

Modern legal regulation of the use of force begins with the U.N. Charter, specifically Article 2(4). That provision directs that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[19] Article 51 of the Charter then provides that "[n]othing in the present Charter shall impair the

19. U.N. Charter art. 2, para. 4.

inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations."[20] Although there is significant debate about the scope of the self-defense right to resort to military force, it is generally agreed that Article 51 carves out an exception to Article 2(4)'s otherwise strict prohibition of force,[21] and it is widely understood that "armed attack" is, although closely related, a narrower category than "threat or use of force."[22]

With respect to offensive cyber-capabilities and the U.N. Charter, then, these provisions raise two major issues. First, in terms of Article 2(4), might certain types of cyber-attacks constitute a prohibited "use of force"? This question has to do with whether the existing legal framework imposes significant constraints on hostile cyber-activities. Second, in terms of Article 51, might a cyber-attack give rise to a right to use military force in response?[23] This question raises the additional issue of what remedies are available to states that suffer cyber-attacks or threats of them.

A. *Historical Divides over Charter Interpretation*

Article 2(4)'s express prohibition is both straightforward and ambiguous. It is direct and absolute on its face, yet, as Oscar Schachter observed, "[t]he paragraph is complex in its structure[,] and nearly all of its key terms raise questions of interpretation."[24] As the opening hypothetical helps illustrate, new technologies raise interpretive puzzles with echoes of previous eras.

1. *Force as Armed Violence*

The dominant view in the United States and among its major allies has long been that the Article 2(4) prohibition of force and the complementary Article 51 right of self-defense apply to military attacks or armed violence.[25]

---

20. *Id.* art. 51.

21. *See* THOMAS M. FRANCK, RECOURSE TO FORCE: STATE ACTION AGAINST THREATS AND ARMED ATTACKS 45-52 (2002).

22. *See* Albrecht Randelzhofer, *Article 51*, *in* 1 THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 788, 796 (Bruno Simma ed., 2d ed. 2002). The U.S. position on this issue, which differs from that of many states and authorities, is discussed *infra* Section II.C.

23. For a survey of approaches to these legal questions, see Daniel B. Silver, *Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter*, 76 INT'L L. STUD. 73 (2002). There is continuing debate about whether there is a gap between Articles 2(4) and 51, insofar as a use of force prohibited by Article 2(4) might not be sufficient to trigger a right to use military force in self-defense. *See* Randelzhofer, *supra* note 22, at 790.

24. Oscar Schachter, *The Right of States To Use Armed Force*, 82 MICH. L. REV. 1620, 1624 (1984).

25. *See* NRC COMMITTEE REPORT, *supra* note 4, at 253 ("Traditional [law of armed conflict] emphasizes death or physical injury to people and destruction of physical property as criteria for the definitions of 'use of force' and 'armed attack.'"); Tom J. Farer, *Political and Economic Coercion in Contemporary International Law*, 79 AM. J. INT'L L. 405, 408-09 (1985) (describing two main interpretations of Articles 2(4) and 51, and arguing that only the one wherein "the only justification for force is prior (or imminent) armed force by one's adversary" is logically sound); Albrecht Randelzhofer, *Article 2(4)*, *in* 1 THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, *supra* note 22, at 112, 117 (noting that the term "force," as used in Article 2(4) is, "according to the correct and prevailing view, limited to armed force"); Bert V. A. Röling, *The Ban on the Use of Force and the U.N. Charter*, *in* THE CURRENT LEGAL REGULATION OF THE USE OF FORCE 3, 3 (A. Cassese ed., 1986) ("It seems obvious to

The plain meaning of the text supports this view, as do other structural aspects of the U.N. Charter. For example, the Charter's preamble sets out the goal that "*armed* force . . . not be used save in the common interest."[26] Similarly, Articles 41 and 42 authorize, respectively, the Security Council to take actions not involving armed force and, should those measures be inadequate, to escalate to armed force.[27] Moreover, Article 51 speaks of self-defense against "armed" attacks.[28] There are textual counter-arguments, such as that Article 51's more specific limit to "armed attacks" suggests that drafters envisioned prohibited "force" as a broader category not limited to particular methods. However, the discussions of means throughout the Charter and the document's negotiating history strongly suggest the drafters' intention to regulate armed force differently and more strictly than other coercive instruments.[29] This interpretation has generally prevailed over alternatives outlined below.

Under the strictest version of this approach, only the first scenario described above—a military strike against Iranian banking facilities—could violate Article 2(4) (unless it were authorized by the Security Council or justified as self-defense) or could itself give rise to a right of armed self-defense.[30] The other scenarios (financial regulatory measures, covert economic disruptions, or computer network attacks) may or may not be unlawful under international law for other reasons,[31] but only the first involves an attack with military violence.

2. *Force as Coercion*

Another view of Article 2(4) reads its purpose more expansively and looks not at the instrument used but its general effect: that it prohibits coercion. Armed force is only one instrument of coercion, and the easiest to identify. This interpretation of Article 2(4) stresses its purpose over its text. At various times, some states—usually those of the developing world, and, during the Cold War, often with Soviet bloc support[32]—pushed the notion that "force"

---

the present writer that the 'force' referred to in Art. 2(4) is military force.").

26. U.N. Charter pmbl. (emphasis added).

27. *Id.* arts. 41-42.

28. *Id.* art. 51.

29. *See* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 905 (1999); *see also* Marco Roscini, *World Wide Warfare—*Jus ad Bellum *and the Use of Cyber Force*, 14 MAX PLANCK Y.B. UNITED NATIONS L. 85, 105 (2010) (noting that early Charter history and "[t]he *travaux préparatoires* also reveal that the drafters did not intend to extend the prohibition to economic coercion and political pressures.").

30. Although this example raises a separate legal question as to whether such an attack on civilian infrastructure would violate the *jus in bello* principle of distinction, as previously mentioned this Article focuses on *jus ad bellum* issues.

31. *See infra* note 60; *see also* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 202 (June 27) ("The principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference. . . . Expressions of an *opinio juris* regarding the existence of this principle . . . are numerous . . . .").

32. For an influential Soviet perspective, see GRIGORI TUNKIN, LAW AND FORCE IN THE INTERNATIONAL SYSTEM (Progress Publishers trans., 1985). Tunkin wrote that "[i]n the literature of socialist states on international law a broad interpretation of force is defended, while a narrow interpretation of that concept prevails in the literature of capitalist states according to which 'force' in

includes other forms of pressure, including political and economic coercion threatening to state autonomy.[33] Debates similar to that over the definition of "force" and "armed attack" in Articles 2(4) and 51 have played out in the U.N. General Assembly over the definition of "aggression," with the United States and its Western allies pushing a narrow definition focused on military attacks, and developing states pushing an expansive definition including other forms of coercion or economic pressure.[34]

Under this approach, any or all of the four hypothesized scenarios could conceivably constitute prohibited "force." Each is intended and is likely to exert coercive pressure on Iran to forego its nuclear ambitions by exacting or threatening crippling costs to its financial sector. A further extension of this approach might go so far as to say that economic coercion could be so intense as to justify armed force in self-defense under Article 51.[35] One problem with this approach has always been the difficulty of distinguishing unlawful coercion from lawful pressure. After all, coercion in a general sense is ever-present in international affairs and a part of everyday diplomacy and statecraft.[36]

3. *Force as Interference*

A third possible approach to interpreting Articles 2(4) and 51 would focus on the violation and defense of rights—specifically, a state's right of sovereign dominion. Such an approach ties the concept of force to improper interference with the rights of other states, focusing on the object and specific character of a state's actions rather than a narrow set of means or their coercive effect.[37] The

---

the sense employed in the United Nations Charter refers only to armed force." *Id.* at 82. He went on to write that "[t]here is no doubt that the use of economic force, for example, by one or more states against one or more other states may represent a very considerable threat to the political independence of states, particularly if they are small, and may produce a significant destabilisation of international relations . . . ." *Id.* However, the Soviet bloc did not always side with the developing world on these questions: "[I]n the realm of force two groupings (socialist and developing countries) tend to agree only up to a point, whereas on certain issues the goals and interests of the USSR coincide with those of the U.S. and a few Western Great Powers." Antonio Cassese, *Return to Westphalia? Considerations on the Gradual Erosion of the Charter System*, *in* THE CURRENT LEGAL REGULATION OF THE USE OF FORCE, *supra* note 25, at 505, 508.

33. *See* AHMED M. RIFAAT, INTERNATIONAL AGGRESSION: A STUDY OF THE LEGAL CONCEPT 120, 234 (1980); Hans Kelsen, *General International Law and the Law of the United Nations*, *in* THE UNITED NATIONS: TEN YEARS' LEGAL PROGRESS 1, 5 (1956) ("It is . . . quite possible to interpret this provision to mean the Members are forbidden not only to use armed force, but also non-armed force constituted by an illegal action directed against another Member without its consent . . . ."); Randelzhofer, *supra* note 22, at 118 ("The developing countries and formerly the Eastern bloc countries have repeatedly claimed that the prohibition of the use of force also comprises other forms of force, for instance, political and, in particular, economic coercion.").

34. *See* JULIUS STONE, CONFLICT THROUGH CONSENSUS 115-36 (1977).

35. *See* Oscar Schachter, *In Defense of International Rules on the Use of Force*, 53 U. CHI. L. REV. 113, 121-44 (1986) (discussing pressures to revise the limits on self-defense drawn by the U.N. Charter but arguing against moves to do so).

36. *See* Farer, *supra* note 25, at 406; Alexander L. George, *Coercive Diplomacy: Definition and Characteristics*, *in* THE LIMITS OF COERCIVE DIPLOMACY 7, 7-11 (Alexander L. George & William E. Simons eds., 2d ed. 1994).

37. As Quincy Wright explained in 1960:

> Domain, like property in systems of national law, implies the right to use, enjoy and transfer without interference from others, and the obligation to each state to respect the

issue of "subversive intervention," or interference with other states' political systems, was of particular concern in the U.N. General Assembly during the early Cold War.[38] States advocating expansive interpretations of prohibited force that would include subversion sought to hermetically seal their domestic system from outside interference while still participating in the broader international political community. In a similar way, some states today want the benefits of international informational connectivity while insulating their computer and communication networks from outside influences or intrusions deemed hostile or undermining.

Reading Article 2(4)'s prohibition of force to include such intrusion into another sovereign's domain would lead to the conclusion that the fourth scenario above—cyber-attack—is equally prohibited as the first and third—military attacks and covert financial intrusion.[39] The second—financial sanctions—might be excluded from the prohibition on the ground that the United States has its own sovereign right to choose with whom it wants to conduct commerce.

Like past efforts to define Article 2(4) "force" as coercion, efforts to expand its coverage beyond armed force so as to include violations of sovereign domain such as propaganda or political subversion never gained significant traction.[40] Pragmatic considerations precluded the much broader interpretation,[41] though this alternative approach raises the question of whether cyber-attacks might be analogized to other covert efforts, like propaganda campaigns, to undermine political or economic systems.[42]

> domain of others. The precise definition of this obligation is the major contribution which international law can make toward maintaining the peaceful co-existence of states.

Quincy Wright, *Subversive Intervention*, 54 AM. J. INT'L L. 521, 528 (1960).

38. *See* Declaration on the Inadmissibility of Intervention into the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, G.A. Res. 2131, ¶¶ 1-2, U.N. GAOR, 20th Sess., Supp. No. 14, U.N. Doc. A/6014, at 12 (Dec. 21, 1965) ("[A]ll . . . forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are condemned. . . . No State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights or to secure from it advantages of any kind.").

To be sure, the United States and other states were not always completely consistent in their interpretations, especially in light of the geostrategic context. An early crisis for the United States involved alleged Yugoslavian, Albanian, and Bulgarian support for guerrilla movements inside U.S.-allied Greece. In seeking U.N. Security Council consideration of the issue, the U.S. ambassador explained that "[i]nvasion by organized armies is not the only means for delivering an attack against a country's independence. Force is effectively used today through devious methods of infiltration, intimidation and subterfuge." U.N. SCOR, 2d Year, 147th mtg. at 1120, U.N. Doc. S/360 (1947).

39. *Cf. Summary Records of the 56th Meeting*, [1950] 2 Y.B. INT'L L. COMM'N 123-24, U.N. Doc. A/CN.4/25 (discussing whether fomenting civil strife could constitute aggression).

40. Wright, *supra* note 37, at 529 ("It is clear that [its provisions] prohibit only the threat or use of armed force or an armed attack. They cannot be construed to include other hostile acts such as propaganda, infiltration or subversion.").

41. *See* FRANCK, *supra* note 21, at 75 ("[D]uring the Cold War, a fairly bright line may be said to have been drawn between . . . a state's export of revolution by direct or indirect military action . . . and . . . a state's export of revolution by propaganda, cultural subversion, and other non-military assistance."); Wright, *supra* note 37, at 529-30.

42. For a discussion of international law regulating covert political and economic activities, see Lori Fisler Damrosch, *Politics Across Borders: Nonintervention and Nonforcible Influence over Domestic Affairs*, 83 AM. J. INT'L L. 1 (1989).

B. *Cyber-Threats and Emergent U.S. Interpretation*

To whatever extent Article 2(4)'s meaning was settled and stable by the end of the Cold War, and to the extent that this meaning generally favored a narrow focus on military violence, cyber-warfare will challenge and test the Charter's bounds. Offensive cyber-attack capabilities, such as inserting malicious computer code to take down public or private information systems or functions that rely on them, bear some similarities to kinetic military force, economic coercion, and subversion. At the same time, cyber-attacks also have unique characteristics and are evolving rapidly and in unpredictable ways.

To deal with these challenges, some scholars and policy experts emphasize the need for clarity in interpreting Articles 2(4) and 51's application to cyber-attacks.[43] Government officials considering offensive and defensive options need to understand legal bounds and risks, the argument often goes.[44] Others emphasize the need for new legal instruments, reasoning that the ambiguity or indeterminacy of Charter provisions and *jus ad bellum* doctrine as applied in this context is best solved through more specific treaty law.[45] Such efforts might build on the International Convention on Cybercrime, adopted in 2001 by the Council of Europe and open to nonmember states, which requires parties to develop criminal laws against hacking and other illicit cyber-activities like computer fraud.[46] A new treaty might, for example, prohibit certain additional categories of hostile cyber-activities or provide for particular remedies.

The United States government has not publicly articulated a general position on cyber-attacks and Articles 2(4) and 51.[47] In the meantime, there is considerable momentum among American scholars and policy experts behind the idea that some cyber-attacks ought to fall within Article 2(4)'s prohibition of "force" or could constitute an "armed attack," at least insofar as those terms should be interpreted to cover attacks with features and consequences closely resembling conventional military attacks or kinetic force. A National Research

---

43. *See, e.g.*, LAWRENCE T. GREENBERG, SEYMOUR E. GOODMAN & KEVIN J. SOO HOO, INFORMATION WARFARE AND INTERNATIONAL LAW 14-19 (1998); James A. Lewis, *Multilateral Agreements To Constrain Cyberconflict*, ARMS CONTROL TODAY, June 2010, at 16 (arguing that states should develop mutual understandings on "what actions can be considered a violation of sovereignty, on what constitutes an act of war, and what actions are seen as escalatory").

44. *See, e.g.*, Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUR. J. INT'L L. 825, 863-64 (2001).

45. *See, e.g.*, ROBERT K. KNAKE, COUNCIL ON FOREIGN RELATIONS, INTERNET GOVERNANCE IN AN AGE OF CYBER INSECURITY 21-23 (2010) (recommending that the United States pursue international legal agreements to limit cyber-attacks); Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023 (2007) (arguing that new international legal regimes or instruments are needed to regulate cyber-operations); Silver, *supra* note 23, at 94 (calling for a new international convention to regulate cyber-attacks).

46. Convention on Cybercrime, Council of Europe, *done* Nov. 21, 2001, E.T.S. No. 185 (entered into force Jan. 7, 2004). A list of Council of Europe member states as well as nonmember states that have signed or ratified the Convention (including the United States) is available at *Convention on Cybercrime, CETS No.: 185*, COUNCIL OF EUROPE, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=28/10/2010&CL=ENG (last visited Apr. 23, 2011).

47. However, one would presume that the U.S. government's actions are guided internally by legal determinations developed through the interagency process.

Council committee charged with studying the issue concluded that cyber-attacks should be judged under the U.N. Charter and customary *jus ad bellum* principles by incorporating analysis of whether the *effects* of cyber-attacks are tantamount to a military attack.[48] Michael Schmitt, in an influential article on the topic, proposes that whether a cyber-attack constitutes force depends on multiple factors derived from what historically made military force special in international law, including severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy.[49] Some policy experts have come to similar conclusions regarding U.S. defensive doctrine against cyber-attacks, emphasizing that the permissibility and appropriateness of military responses to cyber-attacks should turn at least in part on their effects or consequences.[50]

Statements by senior U.S. government officials have either hinted strongly that the United States would regard some cyber-attacks as prohibited force or declined to rule out that possibility—though the U.S. government has not formalized a definitive public position on the issue or articulated clear lines or standards.[51] This suggests that at least one prong of the U.S. strategy may involve a classic military defense and deterrence model, in which the United States would consider the first use of some types of cyber-attacks generally off-limits except in self-defense, and would consider military responses to some cyber-attacks by others.[52] A 1999 Defense Department *Assessment of*

48. *See* NRC COMMITTEE REPORT, *supra* note 4, at 33-34; *see also* Abraham D. Sofaer, David Clark & Whitfield Diffie, *Cyber Security and International Agreements*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 179, 185 (2010), *available at* http://www.nap.edu/openbook.php?record_id =12997&page=179 ("[T]he right of states to exercise self-defense or to take countermeasures in response to such attacks would depend on their potential consequences.").

49. *See* Schmitt, *supra* note 29, at 914-15; *see also* Horace B. Robertson, Jr., *Self-Defense Against Computer Network Attack Under International Law*, 76 INT'L L. STUD. 121, 140 (2002) ("[T]he term 'armed attack' may also include attacks upon computer networks solely by electronic means if the *consequences* of such attacks include either substantial harm to vital civil or military networks, or loss of human life, or both."). For an Estonian view along similar lines, which is interesting because of the country's experience in this area, see Erik Kodar, *Computer Network Attacks in the Gray Areas of* Jus ad Bellum *and* Jus in Bello, 9 BALTIC Y.B. INT'L L. 133, 139 (2009) ("The consequences of [computer network attacks] should be assessed case-by-case to ascertain whether they are similar to the consequences of an armed attack or whether consequences stay below the level of threshold for use of force.").

50. *See, e.g.*, RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR 178 (2010) (proposing a doctrine of "*cyber equivalency*, in which cyber attacks are to be judged by their effects, not their means. They would be judged as if they were kinetic attacks, and may be responded to by kinetic attacks, or other means."); Lewis, *supra* note 43, at 16 ("Agreement on what constitutes an act of war in cyberspace would be helpful. This could be defined as any action that produced an effect equivalent to an armed attack using kinetic weapons."); Silver, *supra* note 23, at 92-93 (discussing effects-based analysis); David Tubbs, Perry G. Luzwick & Walter Gary Sharp, Sr., *Technology and Law: The Evolution of Digital Warfare*, 76 INT'L L. STUD. 7, 15 (2002) ("Until a legal regime matures that comprehensively address State activities in cyberspace . . . legal advisers must principally conduct an effects-based analysis of international law to determine the lawfulness of State activities in cyberspace.").

51. *See* GOV'T ACCOUNTABILITY OFFICE, UNITED STATES FACES CHALLENGES IN ADDRESSING GLOBAL CYBERSECURITY AND GOVERNANCE 38-39 (2010); *see also* William Matthews, *DoD Expanding Domestic Cyber Role*, DEFENSENEWS (Oct. 20, 2010), http://www.defensenews.com/ story.php?i=4939254&c=POL&s=TOP (discussing legal and conceptual uncertainties about cyber-attacks inside the U.S. defense establishment).

52. *See* Mark Clayton, *The New Cyber Arms Race*, CHRISTIAN SCI. MONITOR (Mar. 7, 2011), http://www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-arms-race (quoting former U.S.

International Legal Issues in Information Operations noted:

> If we focused on the means used, we might conclude that electronic signals imperceptible to human senses don't closely resemble bombs, bullets or troops. On the other hand, it seems likely that the international community will be more interested in the consequences of a computer network attack than in its mechanism.[53]

The report went on to suggest that cyber-attacks could constitute armed attacks giving rise to the right of military self-defense.[54]

More recent U.S. government statements amplify that report's logic. Secretary of State Hillary Clinton in 2010 declared the United States's intention to defend its cyber-security in terms similar to those usually used to discuss military security and self-defense:

> States, terrorists, and those who would act as their proxies must know that the United States will protect our networks. . . . [Those who] engage in cyber attacks should face consequences and international condemnation. In an interconnected world, an attack on one nation's networks can be an attack on all.[55]

In testifying before the Senate Committee considering his nomination to head the new Pentagon Cyber Command, Lieutenant General Keith Alexander explained 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."[56] He went on to suggest, however, that "[i]f the President determines a cyber event does meet the threshold of a use of force/armed attack, he may determine that the activity is of such scope, duration, or intensity that it warrants exercising our right to self-defense and/or the initiation of hostilities as an appropriate response."[57]

---

government officials stating U.S. intentions to respond to some cyber-attack scenarios with armed force).

53. U.S. DEP'T OF DEF., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 18 (1999), *available at* http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf, *reprinted in* 76 INT'L L. STUD. 459, 483 (2002). The document goes on to conclude:

> It is far from clear the extent to which the world community will regard computer network attacks as "armed attacks" or "uses of force," and how the doctrines of self-defense and countermeasures will be applied to computer network attacks. The outcome will probably depend more on the consequences of such attacks than on their mechanisms.

Id. at 25; *see also* John Markoff, *Step Taken To End Impasse Over Cybersecurity Talks*, N.Y. TIMES, July 17, 2010, at A7 (quoting a foreign diplomat, who stated that "[t]he U.S. put forward a simple notion that we hadn't said before . . . [that] [t]he same laws that apply to the use of kinetic weapons should apply to state behavior in cyberspace.").

54. *See* U.S. DEP'T OF DEF., *supra* note 53, at 25.

55. Hillary Rodham Clinton, U.S. Sec'y of State, Remarks at the Newseum in Washington, D.C. (Jan. 21, 2010), *available at* http://www.state.gov/secretary/rm/2010/01/135519.htm.

56. *Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command: Before the S. Armed Services Comm.*, 111th Cong. 11 (Apr. 15, 2010), *available at* http://armed-services.senate.gov/statemnt/2010/04%20April/Alexander%2004-15-10.pdf.

57. *Id.* at 12; *see also Military Asserts Right To Return Cyber Attacks*, CBS NEWS (Apr. 14, 2010), http://www.cbsnews.com/stories/2010/04/14/ap/cabstatepent/main6394031.shtml (quoting Lieutenant General Alexander as asserting that while "this right has not been specifically established by legal precedent to apply to attacks in cyberspace, it is reasonable to assume that returning fire in

In addition to these statements, from which we can draw some inferences about the U.S. government's legal and strategic thinking, the U.S. government is reportedly considering a cyber-security strategy that may include preemptive cyber-strikes, designed under certain circumstances to knock out adversaries' computer systems and networks perceived as hostile.[58] This strategy suggests that in addition to the more traditional military defense and deterrence strategies just described, the U.S. government may also be considering legal interpretations flexible enough to permit its own offensive cyber-operations below a certain threshold or against inchoate hostile cyber-activities.[59] Depending on the context and details, other international legal constraints might come into play, though, and the United States also may be prepared in some cases to go beyond the lines it draws for others. For reasons discussed below, the U.S. government is probably concluding that it cannot rely very heavily on traditional forms of military deterrence. Strategies and accompanying interpretations that include possible preemptive cyber-operations are a way of supplementing the United States's defensive strategy with additional layers.[60]

If these inferences about U.S. government strategic thinking are correct, the U.S. government probably prefers an effects- or consequences-based interpretation of "force" or "armed attack" with respect to cyber-attacks not only for what it includes (and therefore what the Charter prohibits and what could trigger self-defense rights), but also for what it excludes. Computer-based espionage, intelligence collection, or even some preemptive cyber-operations or

---

cyberspace, as long as it complied with law of war principles . . . would be lawful."). The same article goes on to report Lieutenant General Alexander as noting "that there is no international consensus on the definition of use of force, in or out of cyberspace" and that "uncertainty creates the potential for disagreements among nations." *Id.*

Meanwhile, the North Atlantic Treaty Organization (NATO) has been working on a joint approach to cyber-security, though NATO's official rhetoric in the field of self-defense has been quite cautious. *See* North Atlantic Treaty Org., *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*, ¶ 19 (2010), *available at* http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf (discussing the need to develop joint policies on cyber-defense); Admiral James Stavridis, Supreme Allied Commander Europe, Address to Armed Forces Communications and Electronics Association (Feb. 2, 2010), *available at* http://www.aco.nato.int/page27750625.aspx (asking whether NATO's reciprocal alliance protection guarantees might be extended to cyber-attacks). The British government's public posture has also been cautious with respect to cyber-security and issues of force, though the government declared in 2009 that "[j]ust as in the 19th century we had to secure the seas for our national safety and prosperity, and in the 20th century we had to secure the air, in the 21st century we also have to secure our advantage in cyber space." U.K. OFFICE OF CYBER SEC., CYBER SECURITY STRATEGY OF THE UNITED KINGDOM 5 (2009).

58. *See* Ellen Nakashima, *U.S. Eyes Preemptive Cyber-Defense Strategy*, WASH. POST, Aug. 29, 2010, at A5; Gene J. Koprowski, *Pentagon Launches Salvo in War To Protect an Army of 7 Million*, FOXNEWS.COM (June 15, 2010), http://www.foxnews.com/scitech/2010/06/15/pentagon-cyber-command-cyber-war/.

59. *See* Ellen Nakashima, *Pentagon Is Debating Cyber-Attacks*, WASH. POST, Nov. 6, 2010, at A1 ("The Pentagon's new Cyber Command is seeking authority to carry out computer network attacks around the globe to protect U.S. interests, drawing objections from administration lawyers uncertain about the legality of offensive operations.").

60. These activities might implicate sources of international law other than the U.N. Charter, however, including the laws of neutrality, customary international law principles related to sovereignty, and rules related to countermeasures. Thus, the U.S. interpretation of Article 2(4) will not occur in a vacuum, and even a flexible interpretation of Article 2(4) may not leave U.S. cyber-operations unconstrained as a matter of international law.

countermeasures designed to disable an adversary's threatening capabilities, for example, would generally not constitute prohibited force because these activities do not produce destructive consequences analogous to a kinetic military attack.[61] Experts inside and outside the government widely agree that the United States is especially strong relative to other states with respect to its ability to penetrate and collect information from others' systems.[62] Consequently, while very concerned about U.S. vulnerabilities to these activities and eager to prevent them, U.S. planners may be reluctant to draw boundaries too tight, lest those boundaries impede their own ability to infiltrate and extract information from others' systems or to prepare to knock out hostile systems in advance of full-fledged attacks. Of course, efforts to draw clear lines between these efforts regarded as short of "force" and prohibited offensive attacks raise tough questions of how to measure and judge the consequences and causal proximity of hostile intrusions, as well as tough technical questions of distinguishing intelligence collection (e.g., extraction of data or mapping foreign information systems) from initiation of offensive operations (e.g., installing malicious code intended to disrupt those systems). In cyberspace, these activities may look identical, especially in real time.[63]

The main alternatives to assessing "force" by reference to effects (or looking to specific sub-factors, such as magnitude, immediacy, and directness) have significant drawbacks. These drawbacks probably weaken their attractiveness to the U.S. government, though Section IV.B below highlights some counter-dangers often neglected in the government's limited public pronouncements and by advocates of defining force in terms of its effects. Along a spectrum of alternatives, at one end, one might take a very legally restrictive view of cyber-attacks. Although I am not aware of any serious proposal that cyber-attacks categorically could *never* constitute "force" or an "armed attack," some legal experts have suggested that to so qualify a cyber-attack must produce "*violent* consequences."[64] Presumably, this would mean that causing a major power system to explode by infiltrating and disrupting its computer control system might constitute force or armed attack, but causing it to shut down by the same means—even for a long time—probably would not. This view places heavy emphasis on the mechanism used to produce harmful

61. *See* NRC COMMITTEE REPORT, *supra* note 4, at 259-61. As a general matter, international law has very little to say about intelligence collection. *See* Sean P. Kanuck, *Information Warefare: New Challenges for Public International Law*, 37 HARV. INT'L L.J. 272, 275-76 (1996); *see also* Jeffrey H. Smith, *State Intelligence Gathering and International Law: Keynote Address*, 28 MICH. J. INT'L L. 543, 544 (2007) ("[B]ecause espionage is such a fixture in international affairs, it is fair to say that the practice of states recognizes espionage as a legitimate function of the state, and therefore it is legal as a matter of customary international law.").

62. *See* Kim Zetter, *Former NSA Director: Countries Spewing Cyber Attacks Should Be Held Responsible*, WIRED (July 29, 2010, 3:52 PM), http://www.wired.com/threatlevel/2010/07/hayden-at-blackhat/ (quoting former NSA Director Michael Hayden as saying that "the U.S. military doesn't consider intelligence attacks acts of war but the kind of 'normal espionage thing that routinely happens between states,'" and that "[w]ithout going into great detail, we're actually pretty good at this, and the Chinese aren't the only ones doing this").

63. *See* NRC COMMITTEE REPORT, *supra* note 4, at 121-126, 135-42.

64. *See, e.g.*, Dinstein, *supra* note 16, at 103 ("The crux of the matter is not the medium at hand . . . but the *violent consequences* of action taken." (emphasis added)).

effects,[65] and it implies that a state facing cyber-attacks could take countermeasures of its own against most attacks in cyberspace but could not resort to *armed* self-defense. A significant problem with this view is that in a world of heavy economic, political, military, and social dependence on information systems, the "nonviolent" harms of cyber-attacks could easily dwarf the "violent" ones. Consider, for example, a take-down of banking systems, causing cascades of financial panic, or the disabling of a power grid system for an extended period of time, causing massive economic disruption and public health emergencies.[66]

At the other end of the spectrum, one might take a very broad view of cyber-attacks and argue that any cyber-attacks of certain types (such as those targeting critical infrastructure like power grids) constitute per se prohibited force or an armed attack.[67] This interpretation is premised on the notion that modern society and its reliance on information systems are such that nonmilitary means can often cause much more harm and pose greater threats than military ones.[68] A significant problem with this view is that it fails to draw a principled distinction between cyber-attacks and other nonmilitary political or economic interference, which can also cause significant harm.[69]

The apparently emergent U.S. view lies between these positions, trying to account in a principled way for the destructive potential of cyber-operations without radically expanding the Charter's scope. However, because the main bureaucratic actors have divergent policy priorities amid a rapidly evolving strategic environment, it probably has been and likely will remain difficult for the U.S. government to develop and articulate clear legal positions on what sorts of actions in cyberspace constitute illicit force. Some parts of the government prioritize the integrity of U.S. military capabilities, while others prioritize protecting U.S. civilian infrastructure, including that of the private sector; some parts seek to prevent any cyber-attacks by establishing high normative barriers to any hostile cyber-activity, while others seek to prevent cyber-attacks through preemptive cyber-attacks of their own; some parts prioritize intelligence collection, often involving infiltration of foreign computer networks and information systems, while others are focused on transnational law enforcement and promoting cooperation.[70] Even if the United

65. *See* David E. Graham, *Cyber Threats and the Laws of War*, 4 J. NAT'L SECURITY L. & POL'Y 87, 91 (2010).

66. *See* NRC COMMITTEE REPORT, *supra* note 4, at 253-54 (arguing that the traditional legal emphasis on death or physical damage is problematic because "modern society depends on the existence and proper functioning of an extensive infrastructure that itself is increasingly controlled by information technology," and that therefore "[a]ctions that significantly interfere with the functionality of that infrastructure can reasonably be regarded as uses of force, whether or not they cause immediate physical damage").

67. *See, e.g.*, WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 140 (1999) ("*Any* computer network attack that intentionally causes *any* destructive effect within the sovereign territory of another state is an unlawful use of force within the meaning of Article 2(4) that may produce the effects of an armed attack prompting the right of self-defense."). Graham calls this a "strict liability" approach. *See* Graham, *supra* note 65, at 91.

68. *See* SHARP, *supra* note 67, at 101-02.

69. *See* Jensen, *supra* note 5, at 224-30 (discussing critiques of Sharp's view).

70. *See* GOV'T ACCOUNTABILITY OFFICE, *supra* note 51, at 38-39 (discussing challenges to

States is generally moving toward an effects-based approach to categorizing cyber-attacks under the U.N. Charter, these divergent policy priorities make it difficult to agree on how broadly or narrowly to draw legal lines, whether to drive toward legal clarity at all, and how actively to engage internationally on these points.

C. *An Interpretive Reorientation*

An approach to overcoming translation problems of Charter rules (which were designed to deal primarily with conventional warfare) that focuses on effects tantamount to a military attack and holds that cyber-attacks *could* constitute force or armed attack is not inconsistent with the narrow interpretations generally advocated by the United States during most of the Charter's history.[71] However, it does represent an argumentative reorientation, since for most of that history the United States was in the position of resisting flexible standards for understanding Article 2(4)'s scope as advocated by those who sought to broaden the Charter's prohibitive scope beyond armed violence. As a result of networked information infrastructures and global economic linkages and supply chains, U.S. security planners now believe the United States has an interest in expanding the Charter, at least at the edges, so as to cover some hostile cyber-activities that might not fit within its traditional understandings of "force" or the triggers of self-defense rights.

Such interpretive reorientation raises subsidiary doctrinal issues that might not sit comfortably with extant U.S. legal positions about the resort to force more generally. For example, in recent years the U.S. government has pushed an interpretation of anticipatory self-defense—the doctrinal notion that a state may resort to self-defensive force in advance of an imminent attack, rather than having to wait to suffer the first blow—that permits flexibility in assessing the "imminence" of a threat so as to take account of the difficulty of assessing when contemporary security threats are temporally immediate.[72] If cyber-attacks with certain effects could give rise to rights of self-defense, could an impending one give rise to such a right in advance as well? Moreover, how would a state even assess imminence in this context?[73] Anticipatory self-defense is especially difficult to evaluate in this context because even if hostile cyber-attack capabilities and intentions are identified, there may be little or no indication of their future timing. It may also be impossible to assess their likely

---

reaching interagency consensus on international legal issues related to cyber-operations); *see also* Ellen Nakashima, *Obama To Name Former Bush, Microsoft Official as Cyber-Czar*, WASH. POST, Dec. 22, 2009, at A4 (discussing challenges of interagency coordination with respect to cyber-defense and operations).

71. *Cf.* IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 362 (1963) (interpreting "use of force" narrowly but looking beyond immediate death or injury from physical impact to the destructive effects).

72. *See* Walter B. Slocombe, *Force, Pre-Emption and Legitimacy*, 45 SURVIVAL 117, 124-25 (2003); William H. Taft IV & Todd F. Buchwald, *Preemption, Iraq, and International Law*, 97 AM. J. INT'L L. 557, 557 n.1 (2003).

73. *See generally* Jensen, *supra* note 5, at 223-39 (discussing anticipatory self-defense doctrine in the context of cyber-threats); Schmitt, *supra* note 29, at 930-34 (same).

consequences in advance, because modern society's heavy reliance on interconnected information systems means that the indirect secondary or tertiary effects of cyber-attacks may be much more consequential than the direct and immediate ones.[74]

Historically, the restrictive U.S. interpretation of the substantive sweep of Article 2(4)'s prohibition and Article 51's self-defense trigger—that they generally apply only to armed violence—was also often paired with a fairly permissive interpretation of Article 51's magnitude threshold, that is, the severity of an attack or threat needed to justify armed self-defense.[75] For example, in the *Oil Platforms* case before the International Court of Justice (ICJ), which concerned the legality of U.S. naval attacks against Iranian oil platforms in the Persian Gulf, the United States argued (unsuccessfully) for a low Article 51 threshold.[76] The United States argued in that case that firing on or mining a vessel could, as a legal matter, be enough to trigger a state's right of armed self-defense,[77] although any force used in response would still be limited legally by the requirement of proportionality.[78] The policy rationale behind the defensively permissive U.S. reading of armed attack thresholds has been that to impose a stricter magnitude-of-attack requirement would irresponsibly tie a state's hands in the face of dangers and encourage antagonists to employ small-scale assaults below that floor.[79] In other words, the U.S. position with respect to the *substantive scope* of Article 2(4)'s prohibition and Article 51's trigger has historically been a narrow one, focused on armed violence, but it has simultaneously advanced a broad view of Article

---

74. *See* David Elliott, *Weighing the Case for a Convention To Limit Cyberwarfare*, ARMS CONTROL TODAY, Nov. 2009, at 21, 24 ("Secondary and tertiary systemic and socioeconomic effects of an attack will often be more important than the initial effect. Because projecting these effects requires difficult-to-obtain specialized knowledge of the interdependence of the systems involved, such estimates will be unreliable.").

75. *See* Abraham D. Sofaer, *Terrorism, the Law, and the National Defense*, 126 MIL. L. REV. 89, 92-93 (1989) ("The United States has always assumed that [Articles 2(4) and 51] . . . make clear that 'force' means physical violence, not other forms of coercion [and] . . . has long assumed that the inherent right of self defense potentially applies against any illegal use of force . . . ."); *see also supra* notes 21-22 and accompanying text (noting a widely held view that differs from that of the United States).

76. Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶¶ 46-77 (Nov. 6).

77. *Id.*; *see also* Harvey Rishikof, *When Naked Came the Doctrine of "Self-Defense": What Is the Proper Role of the International Court of Justice in Use of Force Cases?*, 29 YALE J. INT'L L. 331, 341-42 (2004) (discussing U.S. government thinking regarding the necessity of an armed response during the tanker crisis). The U.S. view is well summarized by William H. Taft IV at the time he served as State Department Legal Adviser, who wrote of the *Oil Platform* decision:

> These statements might be read to suggest that uses of deadly force by a State's regular armed forces, such as the attacks by Iran at issue in this case, do not qualify as an armed attack unless they reach a certain level of gravity. Such a proposition, however, would be inconsistent with well-settled principles of international law.

William H. Taft IV, *Self-Defense and the* Oil Platforms *Decision*, 29 YALE J. INT'L L. 295, 300 (2004). Taft further concluded:

> [T]he Court made statements that might be read as suggesting that the attacks were required to reach some unspecified level of gravity before they would qualify as armed attacks. . . . [That] proposition is [incorrect] as a matter of international law, however, and the United States does not interpret the opinion as relying on [it].

Id. at 299-300.

78. *See* Taft, *supra* note 77, at 303-06.

79. *See id.* at 300-01; Sofaer, *supra* note 75, at 93-96.

51 with respect to the *quantum* of armed violence that would trigger a right to self-defensive military force.[80]

If the United States is reorienting its thinking about the types of actions that would constitute prohibited force or justify self-defensive actions (including military action or its own cyber-operations that others might consider aggressive force), one must wonder whether it might also be recalibrating its view of Article 51's magnitude threshold in this particular context. One possibility would be for the United States to take the position that the magnitude of threat or damage from a cyber-attack must be high to trigger *armed* self-defense (or even constitute prohibited force), while still allowing for self-defensive cyber-operations as necessary countermeasures. The U.S. government statements referred to earlier are ambiguous on this point, but they could be read to suggest that only severe cyber-attacks (measured in terms of effect), as opposed to those causing low levels of harm, could qualify as armed attacks.[81] This would seemingly mark an exception to the United States's general position on Article 51, and therefore establish different thresholds based on instrument of attack: armed violence (low self-defense magnitude threshold) versus cyber-activities (high threshold).

As discussed below, such a threshold differential might make sense from a policy perspective if the goal is to avoid crisis escalation to armed conflict, though a corresponding danger is that it might undermine deterrence of low-level cyber-attacks.[82] If adopted, such analytical moves would represent another subtle but significant interpretive adjustment of U.S. self-defense legal doctrine in light of technological advances.

Another possibility is that the United States will maintain its relatively permissive view that a hostile use of force need not be very severe to trigger self-defense rights across the board, even in cyberspace. Thinking back to the *Oil Platforms* case, the United States could take the position that the cyber-equivalent of laying sea mines would justify armed self-defense. But this then returns to the prior question of when a cyber-attack is legally equivalent to

---

80. The ICJ case *Military and Paramilitary Activities in and Against Nicaragua*, discussed *infra* notes 119-121 and accompanying text, is another such example. In this case, the United States argued that Nicaragua's aggressive support for rebels in El Salvador triggered a right of collective military self-defense. The ICJ rejected that view, holding that Nicaragua's actions were not substantial enough to justify a resort to armed force. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶¶ 187-200, 227-32 (June 27).

81. The 1999 Defense Department legal assessment offers examples of cyber-attacks that would likely constitute armed attacks. The harms in all those examples are hypothesized to be "widespread," "seriously" threaten national security, or interfere with military operations. U.S. DEP'T OF DEF., *supra* note 53, at 15, 18. Lieutenant General Alexander mentioned "scope" and "intensity" as factors likely relevant to self-defense analysis. Alexander, *supra* note 56, at 12. Outside the U.S. government, the National Research Council Report expressly states that cyber-attacks must be severe to trigger self-defense, but that stems from its interpretation of Article 51, under which even kinetic military force only constitutes an "armed attack" if it is sufficiently severe:

> Scale of effect is one important factor in distinguishing between an armed attack and a use of force. For example, an armed attack would presumably involve a use of force that resulted in a large scale of effect. It is unclear if there are other differentiating factors in addition to scale of effect.

NRC COMMITTEE REPORT, *supra* note 4, at 254.

82. *See infra* notes 155-156 and accompanying text.

force at all: when *is* a cyber-attack like deploying sea mines? Again, the few public statements by U.S. government agencies or officials are ambiguous as to whether severity or magnitude is an important or necessary factor in assessing whether cyber-attacks constitute force within the Charter's scope; meanwhile, many scholarly treatments of the issue include severity or magnitude as a factor.[83] The more important severity is to classifying cyber-attacks as force or armed attacks, the more distinct that analysis looks from U.S. interpretations of conventional military attacks, which tend not to put much weight on severity.

* * *

From a U.S. policy standpoint, answering these sorts of interpretive questions is important in order to plan and guide offensive and defensive actions,[84] and it may be useful in signaling U.S. intentions. Although much depends on detailed analysis and application to specific fact patterns, the apparent trajectory of U.S. efforts—inferred from public statements to date that look to cyber-attacks' effects to determine whether they cross U.N. Charter prohibitions or thresholds—represents a reasonable effort to translate foundational rules drawn up for an era of conventional warfare in physical space to a new era of electronic and informational warfare in cyberspace. However, as discussed below, it carries some strategic dangers as well.[85] International lawyers may also object that the apparent interpretive trajectory replaces relatively clear rules that are in many cases easy to administer (because armed violence is generally observable and easy to distinguish from other forms of interstate behavior) with less determinate, blurry tests.[86]

With these questions and concerns about emerging U.S. positions in mind, and looking more broadly at the international legal system as a whole, how likely is it that emergent U.S. interpretations will take hold? Even if they do, how potent will the U.N. Charter be in restraining cyber-attacks? The next Parts take up these questions.

III. CYBER-ATTACKS AND CHANGING MODES OF CONFLICT

In thinking about how future modes of conflict might fit within the U.N. Charter legal regime, it is useful to look backward in time. Other revolutionary changes in the way conflict is waged strained the U.N. Charter during the Cold War, sometimes close to the breaking point. An examination of those changes

83. *See, e.g.*, NRC COMMITTEE REPORT, *supra* note 4, at 254-56 (discussing "scale" of cyber-attacks as a factor in assessing whether cyber-attacks constitute force); Schmitt, *supra* note 29, at 916-17 (discussing severity as a factor in assessing whether cyber-attacks constitute force).

84. *See* Nakashima, *supra* note 58 (reporting that U.S. officials are reluctant to use cyber-weapons until international legal questions are resolved).

85. *See infra* Section IV.B.

86. Fifty years ago, Ian Brownlie wrestled with this issue, too, in arguing that chemical or biological weapons likely could be considered force because they destroy life and property. He was more skeptical about whether the "release of large quantities of water down a valley, and the spreading of fire through a built up area or woodland across a frontier" (either of which might be thought analogous to some cyber-attacks) would constitute force. BROWNLIE, *supra* note 71, at 362-63.

and the legal responses to them highlights how some likely attributes of cyber-attacks—including low visibility of offenses and responses, and difficulties in attributing attacks to their sources or sponsors—will undermine the Charter's constraining influence in this context.

A. *Cold War Conflict and the U.N. Charter*

About midway through the Cold War, Thomas Franck famously lamented the "death" of Article 2(4) in the pages of the *American Journal of International Law*. He believed that rapid changes in the way conflict was waged had made its prohibitions of force obsolete:

> The great wars of the past, up to the time of the San Francisco Conference, were generally initiated by organized incursions of large military formations of one state onto the territory of another, incursions usually preceded by mobilization and massing of troops and underscored by formal declarations of war. Because it was so familiar to them, it was to aggression of this kind that the drafters of Article 51 addressed themselves. Modern warfare, however has inconveniently by-passed these Queensberry-like practices.[87]

Small-scale wars and subversion and counter-subversion waged through local proxies became a common mode of superpower conflict, rather than direct conventional military action.[88] In places such as Greece, Laos, Vietnam, and Lebanon, the superpowers routinely supported insurgencies, rebel movements, and coups against states supporting the other power with various forms of assistance, including arms.[89] Many Latin American and African states also became superpower battlegrounds, fought over through insurgencies and counterinsurgencies.[90] At the same time, the swift and devastating nature of nuclear attacks and the development of nuclear deterrence doctrines meant that major powers were locked in a permanent state of threatened force.[91] In both respects, the "technology" (broadly speaking) and strategy of conflict had moved in directions for which the U.N. Charter's regulatory content and structure were ill equipped.[92]

In retrospect, Franck was half right. Louis Henkin responded—correctly—that Article 2(4) was battered and bruised but not killed: "[T]he death certificate is premature and the indictment for legicide must be redrawn to charge lesser though aggravated degrees of assault."[93] "Even where force is

---

87. Thomas M. Franck, *Who Killed Article 2(4)? Or: Changing Norms Governing the Use of Force by States*, 64 AM. J. INT'L L. 809, 812 (1970); *see also* Michael J. Glennon, *How International Rules Die*, 93 GEO. L.J. 939 (2005) (concluding that Article 2(4) had been violated so frequently that it had fallen into desuetude).

88. Franck, *supra* note 87, at 812-20.

89. *Id.* at 813.

90. *See, e.g.*, John Norton Moore, *Low-Intensity Conflict and the International Legal System*, 67 INT'L L. STUD. 25, 28 (1995).

91. *See* Franck, *supra* note 87, at 820.

92. *See id.* at 820-22; *see also* Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 43 (July 8) (declining to hold the use or threat of using nuclear weapons to be per se unlawful under the U.N. Charter).

93. Louis Henkin, *The Reports of the Death of Article 2(4) Are Greatly Exaggerated*, 65 AM. J. INT'L L. 544, 544 (1971).

used," Henkin continued, "the fact that it is unlawful cannot be left out of account and limits the scope, the weapons, the duration, the purposes for which force is used."[94]

In other words, while it was never really likely to prevent warfare completely without strong supranational institutions powerful and independent enough to enforce it, Article 2(4)'s prohibitions may make aggression less likely and influence the form it takes by raising the costs of some actions. At minimum, the Charter's normative principles constrain states' actions to defend or advance their security interests by shaping the way those actions are justified publicly and perceived and measured against international community expectations, thereby affecting political, diplomatic, and other costs.[95] Some scholars would go further and argue that norms regarding force have more significant internal pull on state decisionmaking, at least among some types of states.[96] In any event, the Charter's basic prohibitions had some strength and resilience through the Cold War because powerful states shared a collective interest in their vitality, especially when any conventional war had the potential for unlimited escalation.[97]

Franck and Henkin were both correct in their approach to assessing Article 2(4)'s continued value. Each looked beyond the question of whether states used "force" at all and instead considered, first, the *way* that states used force, and second, whether Article 2(4)'s ability to impose costs on purported violators could keep pace with changing warfare. Indeed, the costs Article 2(4) imposed on conventional military attacks across borders may even have had substitution effects, pushing actors in the international system toward other modes of conflict.[98] This is similar to the way the United States today may be pushed toward options other than military strikes in the introductory

94. *Id.*

95. *See* ABRAM CHAYES, THE CUBAN MISSILE CRISIS: INTERNATIONAL CRISES AND THE ROLE OF LAW 103-04 (1974); Sean D. Murphy, *The Doctrine of Preemptive Self-Defense*, 50 VILL. L. REV. 699, 702-05 (2005); Matthew C. Waxman, *The Use of Force Against States that* Might *Have Weapons of Mass Destruction*, 31 MICH. J. INT'L L. 1, 53-55 (2009).

96. *See* Thomas H. Lee, *International Law, International Relations Theory, and Preemptive War: The Vitality of Sovereign Equality Today*, 67 LAW & CONTEMP. PROBS. 147, 158 (2004). Others theorize that norms have greater influence on state behavior, particularly over liberal state behavior, when addressing issues pertaining to war and peace. *See* DAVID ARMSTRONG, THEO FARRELL & HÉLÈNE LAMBERT, INTERNATIONAL LAW AND INTERNATIONAL RELATIONS 140 (2007).

97. *See* PAUL GORDON LAUREN, GORDON A. CRAIG & ALEXANDER L. GEORGE, FORCE AND STATECRAFT 95 (4th ed. 2007) ("Every major crisis . . . always was coupled with the fear that *any* shooting war between American and Soviet forces, no matter at how modest a level initially, could escalate completely out of control.").

98. *See* Alberto R. Coll, *Unconventional Warfare, Liberal Democracies, and International Order*, 67 INT'L L. STUD. 3, 3 (1992) ("The high political, military, and economic risks increasingly associated through the course of the twentieth century with open, conventional war have led many States and non-State entities to shift to other forms of violence as instruments of foreign policy."); Alexander L. George & William E. Simons, *Findings and Conclusions*, *in* THE LIMITS OF COERCIVE DIPLOMACY, *supra* note 36, at 267, 272 ("Covert sponsorship or encouragement of internal upheaval and irregular forms of aggression by others . . . makes it difficult for the defenders to clearly define the aggressive behavior and assign political responsibility for that behavior."); Robert F. Turner, *State Sovereignty, International Law, and the Use of Force in Countering Low-Intensity Aggression the Modern World*, 67 INT'L L. STUD. 43, 60 (1992) ("[T]he low-intensity conflict scenario is selected because it provides a colorable claim of legitimacy (being less obvious).").

hypothetical, and the way Stuxnet malware was probably used to attack Iran's nuclear program as a substitute for military options.[99] That is, by heavily regulating some modes of conflict but not others, the law may have pushed antagonists toward the latter.

As information technology opens up new modes of interstate conflict, questions for cyber-warfare include the following: can Article 2(4)'s contours adjust to cyber-capabilities in ways that differentiate illicit conduct from legal activities? Can those changes help impose costs for noncompliance? And in doing so, can they command the respect and support of powerful actors in the international system?

B. *Legal Process, Enforcement Challenges, and "Technologies" of Conflict*

The Cold War history of Article 2(4) teaches several lessons about the effect of new technologies on waging and regulating conflict. First, as new technologies of conflict develop, reaching broad international consensus on interpretation of the U.N. Charter may be slow and difficult. Second, some technologies or modes of conflict will be especially challenging to regulate because their features match poorly with the general enforcement mechanisms of the law regulating force.[100] These mechanisms sometimes include U.N. Security Council processes or other U.N. organs, but more often involve decentralized assessments and evaluations by states, international institutions, and other influential international actors. As Michael Reisman puts it:

> International law is still largely a decentralized process, in which much lawmaking (particularly for the most innovative matters) is initiated by unilateral claim, whether explicit or behavioral. Claims to change inherited security arrangements . . . ignite a process of counterclaims, responses, replies, and rejoinders until stable expectations of right behavior emerge.[101]

One reason why cyber-attacks will be difficult to regulate through such processes is that the factual bases for asserting or contesting a violation of Article 2(4) or a right of armed self-defense under Article 51 will be subject to great uncertainty, debate, opacity, and lack of verifiability.[102] There are technical, legal, and political or strategic reasons for these difficulties.

As a technical matter, those who study the problem of legally regulating cyber-attacks are usually quick to point out the problems of identification and attribution: it is not always possible to discern quickly or accurately who launched or directed an attack.[103] The nature of digital information

---

99. According to former NSA General Counsel Stewart Baker, "It's the first time we've actually seen a weapon created by a state to achieve a goal that you would otherwise have used multiple cruise missiles to achieve." Christopher Dickey et al., *The Shadow War*, NEWSWEEK, Dec. 20, 2010, at 28, 31 (quoting Stewart Baker).

100. *See* Schachter, *supra* note 24, at 1645-46; Waxman, *supra* note 95, at 53-55.

101. W. Michael Reisman, *Assessing Claims To Revise the Laws of War*, 97 AM. J. INT'L L. 82, 82 (2003).

102. For a general discussion of proof standards and self-defense amid factual uncertainty about threats, see Waxman, *supra* note 95, at 57-77.

103. *See* NRC COMMITTEE REPORT, *supra* note 4, at 138-41, 252; Hollis, *supra* note 45, at

infrastructure facilitates anonymity, and adversaries can route their attacks through others' computer systems. Meanwhile, forensics are such that it may be very difficult to link a penetration or disruption of a computer or information networks to the responsible party, though forensic capabilities are generally improving, albeit unevenly across states.[104] Even if individual perpetrators can be identified, it may be difficult to substantiate as a matter of fact on whose behalf they are operating.

These technical issues are exacerbated by jurisdictional concerns. There are jurisdictional limits on any state's ability to investigate beyond its own borders—an especially daunting problem when electronic attacks can include transit computers and networks spanning dozens of countries.[105] As one early study of this problem put it, "Investigators tracing attacks across computer networks may be stymied by a collision between fundamental principles of physics and those of international law, namely that electrons may flow through networks freely across international borders, but the authority of agents of national governments does not."[106]

Moreover, even if investigation processes can trace a cyber-attack back through digital networks to its source, it may be difficult to publicize that information in a timely and convincing way, especially when states or private entities are likely to have strong incentives not to discuss the technical details of informational security breaches or reveal their own capabilities to adversaries or third parties.[107] As a case in point, the U.S. government waited two years before disclosing that in 2008 it suffered "the most significant breach of U.S. military computers ever" when a flash drive inserted into a U.S. military laptop surreptitiously introduced malware into the Pentagon's classified and unclassified computer systems.[108] Even then, the U.S. government disclosed few details about the extent of harm and said nothing about its knowledge of the likely perpetrators.[109] Iran has likewise been very reticent about Stuxnet, its effects, and Iran's knowledge of the code's source.[110]

1031-32; *see also* Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L.J. (forthcoming 2011) (manuscript at 26-33), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1670330& (discussing the attribution problem).

104. For a discussion of the attribution challenges specific to different types of cyber-attacks, including Internet-based attacks, non-Internet cyber-attacks, and threats of malicious code inserted into supply chains, see *Untangling Attribution: Moving to Accountability in Cyberspace, Planning for the Future of Cyber Attack: Hearing Before the H. Subcomm. on Tech. and Innovation of the H. Comm. on Sci. and Tech.*, 111th Cong. (July 15, 2010) (statement of Robert K. Knake, Int'l Aff. Fellow in Residence, Council on Foreign Relations), *available at* http://gop.science.house.gov/Media/hearings/ets10/july15/Knake.pdf.

105. *See* KNAKE, *supra* note 45, at 16 ("Whereas national legal authority is bounded by borders, the Internet is not."); Hollis, *An e-SOS for Cyberspace*, *supra* note 103, at 26-30.

106. GREENBERG ET AL., *supra* note 43, at 23.

107. *See* NRC COMMITTEE REPORT, *supra* note 4, at 138-41.

108. *See* Lynn, *supra* note 5, at 97.

109. *See* Ellen Nakashima, *Defense Official Discloses Cyberattack*, WASH. POST, Aug. 25, 2010, at A3. In 2008, anonymous sources told the *Los Angeles Times* that they suspected the incursion originated in Russia, but they could not be sure whether the program was created by private hackers or whether the Russian government was involved. *See* Julian E. Barnes, *Pentagon Computer Networks Attacked*, L.A. TIMES, Nov. 28, 2008, at A1.

110. *See* Sanger, *supra* note 10, at 4.

Others have noted that the attribution challenges of cyber-attacks pose problems for deterrence (because if you cannot identify the perpetrators, you cannot threaten them)[111] and for enforcing the law (because you cannot hold unidentifiable perpetrators accountable).[112] In addition to those problems, the argument here goes further. Attribution challenges—both the technical aspects and the ability to make those findings public in a credible, persuasive way—as well as the secrecy and low visibility of some states' responsive actions in cyberspace, pose challenges for the substantive development of the law. It will be difficult to develop consensus understandings even of the fact patterns on which states' legal claims and counterclaims are based, assuming those claims are leveled publicly at all.

Put another way, the ability to determine the ultimate perpetrator and sponsor of cyber-attacks may be necessary to take effective defensive or deterrent action, to satisfy a state's legal obligations internally, and to justify a state's responses externally. However, the level of certainty a state requires internally may be different than the level of certainty needed to justify responses externally.

A separate but related problem is the uncertainty of causation, or how to ascribe harms of cyber-attacks. For example, if state *A* disrupts the information network of state *B*'s stock market, resulting in a massive decline in investor confidence with unpredictable ripple effects throughout *B*'s economy, what portion of the ensuing harm ought to be legally attributed to *A*'s actions for *jus ad bellum* purposes? As discussed earlier, modern society's heavy reliance on interconnected information systems means that the indirect and secondary effects of cyber-attacks may be much more consequential than the direct and immediate ones.[113] Once state *B* takes defensive and perhaps offensive countermeasures in cyberspace, it may be especially difficult to untangle the strands of fact, associate them with specific effects, and assign them clear legal significance. Consider the opening hypothetical: if the United States electronically disrupted Iran's banking system, which harms that followed—perhaps days or weeks later—could be ascribed legally to those actions, especially in the context of other overt efforts to weaken Iran's economy with economic sanctions and Iran's own responsive actions?

Again, though, these are not entirely new problems for Article 2(4); the issues of attribution and causality arose many times in Cold War era Article 2(4) debates. As Franck explained, "The small-scale and diffuse but significant and frequent new wars of insurgency have, by their nature, made clear-cut distinctions between aggression and self-defense, which are better adapted to

111. *See* MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR 41-52 (2009); NRC COMMITTEE REPORT, *supra* note 4, at 303 (arguing that "a credible threat to impose costs requires knowledge of the party on which the costs should be imposed" but "attribution of a cyberattack is a very difficult and time-consuming—and perhaps insoluble—problem"); John Markoff, David E. Sanger & Thom Shanker, *In Digital Combat, U.S. Finds No Easy Deterrent*, N.Y. TIMES, Jan. 26, 2010, at A1 (discussing difficulties of determining source of cyber-attacks and challenges for deterrence).

112. *See* NRC COMMITTEE REPORT, *supra* note 4, at 252-53; Jack Goldsmith, *The New Vulnerability*, NEW REPUBLIC, June 24, 2010, at 21, 23.

113. *See supra* note 74 and accompanying text.

conventional military warfare, exceedingly difficult."[114] Moreover:

> While it was not always possible even in classical combat to determine which army had started marching first, the scale, formations and strategy of conventional warfare did make the identification of aggression relatively easy. It stretched everyone's credulity to be told that Poland had attacked Germany or South Korea the North, when the armies of these self-proclaimed victims were, right at the very beginning, to be seen as overrunning their opponents. . . . With the hit-and-run tactics of wars of national liberation, on the other hand, it is often difficult even to establish convincingly, from a pattern of isolated, gradually cumulative events, when or where the first round began, let alone at whose instigation, or who won it.[115]

Whereas conventional wars or attacks of the past were usually easily visible and measurable, unconventional or low-intensity conflict featured inconclusive evidence of foreign involvement or hostile action, and foreign state antagonists worked to mask, conceal, or obscure their participation and responses.[116] In other words, once conflict was waged through proxies, it was difficult to develop international consensus about the relevant facts on such basic issues as what occurred and on whose behalf, let alone consensus about *jus ad bellum* responsibility or justification.[117]

Such legal-factual murkiness helps explain why Article 2(4) seemed unable to address that form of conflict and why that mode of conflict offered an appealing option to the Cold War antagonists.[118] Perhaps to try to bring greater legal clarity and predictability to this situation, the ICJ in *Nicaragua v. United States*,[119] in holding that the United States had violated international law in supporting *Contra* guerrillas and mining Nicaragua's harbors, imposed high bars on the level of violence necessary to constitute an "armed attack" and the level of state control over foreign agents necessary to warrant attribution of their illicit actions.[120] In so doing, the ICJ rejected the United States's claim that it had acted in collective self-defense of El Salvador, responding to Nicaragua's alleged support for rebels there. But, while these doctrinal

---

114. Franck, *supra* note 87, at 820; *see also* Coll, *supra* note 98, at 16 ("Whereas conventional military attacks are susceptible to fairly straightforward processes of inquiry, and hence to authoritative determinations that armed aggression has taken place, unconventional warfare is not.").

115. Franck, *supra* note 87, at 820.

116. *See* Coll, *supra* note 98, at 15 ("By its very nature, unconventional warfare leaves as few trails as possible. Conclusive, incontrovertible evidence of a party's guilt is hard to come by.").

117. Louis Henkin similarly noted in the context of self-defense authority that justifications for armed responses should be limited to armed attacks, "which [are] clear, unambiguous, subject to proof, and not easily open to misinterpretation or fabrication." Louis Henkin, *The United Nations and Its Supporters: A Self-Examination*, 78 POL. SCI. Q. 504, 532 (1963).

118. *See* Coll, *supra* note 98, at 4 ("The covert nature and elusive instrumentalities of unconventional warfare make it difficult for societies under attack to identify the source of the threat and to rally domestic and international opinion . . . . Unconventional warfare places its victims in the awkward legal, moral, and political dilemma of choosing an appropriate response."); *see also* Franck, *supra* note 87, at 817 ("In the absence of some universally credible fact-determination procedures, the effort to establish whether a use of force is illegal under Article 2(4) or legal under Article 51 is stymied by contradictory allegations of fact by the parties to the dispute and their allies.").

119. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14 (June 27).

120. *See* Reisman, *supra* note 101, at 83-84 (describing the ICJ's decision in *Nicaragua* as reflecting the Court's effort to impose high thresholds of violence necessary to justify self-defense).

approaches may have made sense to a court trying to articulate standards that would constrict opportunities for states to militarily escalate conflict, they did little to address the underlying challenges of contemporary interstate conflict being waged through surrogates and unconventional means, and may have even contributed to them.[121]

Like these prior proxy wars, cyber-conflict is likely to feature disputed facts about what exactly occurred, including who committed the electronic disruption and on whose behalf they did it.[122] In some respects, those problems will likely be vastly exacerbated in the cyber-context because of participants' greater ability to mask or anonymize their identity and because the "movements" and "terrain" of cyber-warfare can be dispersed across global information networks and will often be carried out on private infrastructure.[123] "While in most conflicts, both sides claim that they are acting in self-defense, cyber-conflicts are a particularly messy domain in which to air and judge such claims."[124]

Consider again the case of Estonia, referenced earlier,[125] in which information about the source of attacks on Estonian computer networks took months to compile, and many key facts—including ultimate responsibility for directing or encouraging the attacks—remain subject to dispute.[126] Evidence of Russian government involvement was mostly circumstantial, the compromised computers that were harnessed remotely for the attack were located on several different continents, and Russian officials denied involvement.[127] There is also evidence suggesting that the Russian government may have encouraged nongovernmental "patriotic hackers"[128] to conduct attacks, and that China is similarly relying on unofficial, semi-private hackers to maintain deniability.[129]

Utilizing loosely or ambiguously affiliated actors resembles the way Cold War superpowers relied on surrogate forces, though this time arrayed across cyberspace rather than third-party territories.[130] Like proxy warfare, the factual

---

121. *See* John Lawrence Hargrove, *The* Nicaragua *Judgment and the Future of the Law of Force and Self-Defense*, 81 AM. J. INT'L L. 135, 141-43 (1987); John Norton Moore, *The* Nicaragua *Case and the Deterioration of World Order*, 81 AM. J. INT'L L. 151, 152 (1987) (arguing that the ICJ announced "contrary to the Charter, a restrictive interpretation of the right of defense that could deny individual or collective defense against secret warfare, the most serious contemporary threat to world order"); *see also* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 350 (June 27) (Schwebel, J., dissenting) (arguing that the Court's decision could encourage predatory subversion); *id.* at 543-44 (Jennings, J., dissenting) (arguing that the Court's decision dangerously restricts self-defense against support for rebels).

122. *See* Hollis, *supra* note 45, at 1031-32.

123. *See* Kanuck, *supra* note 61, at 286-88.

124. *See* NRC COMMITTEE REPORT, *supra* note 4, at 315.

125. *See supra* notes 8-9 and accompanying text.

126. *See* NRC COMMITTEE REPORT, *supra* note 4, at 173.

127. *See id.*

128. *See* Charles Clover, *Kremlin-Backed Group Behind Estonia Cyber Blitz*, FIN. TIMES, Mar. 11, 2009, at 8.

129. *See* Anne Applebaum, *For Estonia and NATO, a New Kind of War*, WASH. POST, May 22, 2007, at A15; David E. Sanger, John Markoff & Thom Shanker, *U.S. Plans Attack and Defense in Web Warfare*, N.Y. TIMES, Apr. 28, 2009, at A1.

130. With some obvious parallels to this problem, Franck worried in 1970:

Insofar as one state merely encourages guerrilla movements within another, an "armed

haziness surrounding cyber-attacks—and therefore the difficulty in reaching agreement on legal appraisal—may make cyber-attacks an appealing weapon to some states.[131]

* * *

To an even greater degree than the proxy warfare of the Cold War, cyber-warfare may lack clearly discernable starting points and readily observable or provable actions and counter-actions.[132] This does not mean that legal line drawing through U.N. Charter interpretation or new international legal agreements is impossible with respect to issues of prohibited attacks and self-defense. It does mean, however, that while information technology continues to evolve at faster and faster rates, the processes of claims and counterclaims moving toward a predictable, stable outcome, or the accretion of interpretive practice commanding broad consensus, will likely be slow and uncertain.

IV. THE LAW OF CYBER-WARFARE AND THE DISTRIBUTION OF POWER

Besides the specific challenges of regulating certain types of conflict, Cold War experience with U.N. Charter interpretation illustrates important principles about the relationship between law and power that are applicable to a discussion of cyber-capabilities. Competing interpretations of Articles 2(4) and 51 have always reflected distributions of power. As a corollary, efforts to revise legal boundaries and thresholds may have re-allocative effects on power by raising or lowering the costs of using resources and capabilities that are unequally apportioned.[133]

The United States appears to be placing its legal bets on a future world in which it can continue to rely partly on its comparative military edge to deter

---

> attack," at least in the conventional sense, cannot be said to have taken place. The more subtle and indirect the encouragement, the more tenuous becomes the analogy to an "armed attack." Article 51 does not, however, on its face, recognize the existence of these newer modes of aggression, or attempt to deal with the new problems of characterization which they create for international law.

Franck, *supra* note 87, at 812. This issue was also a subject of the ICJ *Nicaragua* litigation, and more recently international tribunals have tried to clarify when aggressive actions by nonstate actors may be attributed to a state sponsor. *See, e.g.*, Prosecutor v. Tadic, Case No. IT-94-1-A, Judgment on Appeal, ¶¶ 115-62 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999) (holding that a foreign state's overall control, rather than effective control, of a nonstate military organization may render that state responsible for acts of the organization and may make applicable international law governing international armed conflicts).

131. Alberto Coll argues that unconventional warfare favored authoritarian state sponsors, "because of their adeptness at deception and manipulation of information, which in turn is facilitated by the closed and secretive nature of their societies." Coll, *supra* note 98, at 17. The same strategic asymmetry might apply to cyber-warfare, due to those same factors as well as some states' strict control of information networks themselves.

132. Unconventional warfare during the Cold War was often used as an instrument of coercive pressure, so while the supporting superpowers wanted to maintain some deniability, they did not want to shield their sponsorship entirely.

133. For a discussion of how power politics influences international legal strategy, see Paul B. Stephan, *Symmetry and Selectivity: What Happens in International Law When the World Changes*, 10 CHI. J. INT'L L. 91 (2009).

cyber-attacks while supplementing that deterrence with its own offensive, defensive, and preemptive cyber-capabilities—a bet that plays to some advantages but also carries risks. Reaching legal consensus with other major powers on these issues will be difficult in part because they perceive a different combination of strategic risks and opportunities. Therefore, U.S. policymakers should prepare to operate in a highly contested and uncertain international legal environment.

A. *Cold War Power Relations and the U.N. Charter*

As discussed above, a major Cold War legal dispute about Article 2(4)—one pitting groupings of the world's states against each other—concerned whether Article 2(4) bans aggressive military violence only, or whether it also covers other forms of coercion, including economic coercion. Some states,[134] along with a few notable international law scholars,[135] argued that Article 2(4) prohibited a much broader category of coercion than just military force. However, this broader position never gained traction as a matter of authoritative practice; the more restrictive interpretation confined to military means won out.

From the perspective of the United States, this seemed like a good bargain: the costs placed by international law on states of resorting first to conventional armed force in a crisis were high, thereby generally helping to preserve territorial stability and prevent escalation.[136] In the meantime, the United States could build its defenses, grow its economy, and expand its influence, all the while relatively free to use its disproportionate economic and diplomatic muscle to pressure smaller states without the fear of reciprocal coercion.[137] (This was the case at least until the Arab states launched an oil embargo in 1973, at which moment that deal may not have seemed so favorable.)[138]

In short, where one stands on interpreting Articles 2(4) and 51 has historically depended on one's share of global resources and power, including whether one is satisfied or unsatisfied with the status quo.[139] Moreover, those

134. *See supra* Section II.A.

135. *See, e.g.*, STONE, *supra* note 34, at 96-101.

136. *See* Tom J. Farer & Christopher C. Joyner, *The United States and the Use of Force*, 1 TRANSNAT'L L. & CONTEMP. PROBS. 15, 23 (1991) ("[During the] Cold War, Washington, despite its still conservative objectives, felt unduly constrained by the Charter's apparent limits on the means for achieving them. Where we could, we stretched those limits with imaginative interpretation, and when we reached the absolute limits of interpretive elasticity, we sometimes evaded them.").

137. *Id.* at 22 ("[A]t the close of World War II, the United States was the archetypal satisfied power. Acquisition of the atomic bomb gave it military preeminence over the Soviet Union. In the economic realm it had no rival.").

138. *See* STONE, *supra* note 34, at 115-36; Jordan J. Paust & Albert P. Blaustein, *The Arab Oil Weapon: A Threat to International Peace*, 68 AM. J. INT'L L. 410 (1974).

139. *Compare* Rosalyn Higgins, *The Attitude of Western States Towards Legal Aspects of the Use of Force*, *in* THE CURRENT LEGAL REGULATION OF THE USE OF FORCE, *supra* note 25, at 435-36 (discussing Western states' desire to keep Charter interpretations on the use of force as the status quo), *with* Milan Sahovic, *Non-Aligned Countries and the Current Regulation on the Use of Force*, *in* THE CURRENT LEGAL REGULATION OF THE USE OF FORCE, *supra* note 25, at 479, 485 (expressing grave concern among non-aligned states with "any form of coercion," not just armed force).

with more power have greater ability to impose their preferred interpretation. As Julius Stone observed of the U.N. Charter in 1977:

> Against the bench-mark of existing international law, particular offered definitions may tend to preserve the *status quo* of distribution. Or they may drive drastically to change or revolutionise this distribution. From the standpoint of proponents of a particular content, it is likely to favour the *status quo* as to those resources in which the proponent is affluent; and to support change or revolution as to those of which it regards itself as deprived. What an offered definition *with any substantive content* can rarely be, is merely neutral about the disposal of world resources.[140]

Myres McDougal and Florentino Feliciano, whose policy-oriented approach to global public order also emphasized a broader interpretation of legal prohibitions than did more mechanical or formalist accounts,[141] also emphasized the relationship between power distribution and prohibited force line drawing. Specifically, they stressed that difficulties in distinguishing lawful from unlawful coercion are "greatly magnified in the global community by gross inequalities in the distribution of effective power."[142]

B. *Technology, Power Shifts, and the Strategic Logic of Legal Interpretation*

With these relationships between law and power in mind, the United States has an interest in regulating cyber-attacks, but it will be difficult to achieve such regulation through international use-of-force law or through new international agreements to outlaw types of cyber-attacks.[143] That is because the distribution of emerging cyber-capabilities and vulnerabilities—vulnerabilities defined not only by the defensive capacity to block actions but also by the ability to tolerate and withstand attacks—is unlikely to correspond to the status quo distribution of power built on traditional measures like military and economic might.

---

140. STONE, *supra* note 34, at 110.

141. MYRES S. MCDOUGAL & FLORENTINO P. FELICIANO, THE INTERNATIONAL LAW OF WAR: TRANSNATIONAL COERCION AND WORLD PUBLIC ORDER 259 (1994) (arguing that prohibitions on force are "most rationally conceived as extending to all coercion, by whatever instrument or combination of instruments, military and other, which is directed with requisite intensity against such substantial bases of power as the 'territorial integrity' and 'political independence' of the target state"); *see also* W. Michael Reisman, *Coercion and Self-Determination: Construing Charter Article 2(4)*, 78 AM. J. INT'L L. 642, 644 (1984) (criticizing the restrictive "rule formulation" of Article 2(4) as inappropriately tailored to the policy ambitions of international law).

142. Myres S. McDougal & Siegfried Wiessner, *Introduction to the Reissue* of MCDOUGAL & FELICIANO, *supra* note 141, at xix, xxxiv.

143. Many policy experts and some legal scholars have advocated new international agreements of this sort. *See, e.g.*, KNAKE, *supra* note 45, at 21-23 (proposing a U.S. strategy for negotiating international limits on cyberwarfare); Shackelford, *supra* note 9, at 197-98 (advocating a new international accord on cybersecurity); Silver, *supra* note 23, at 94 ("[E]fforts should be made towards the adoption of an international convention that would bind the parties not to use [computer network attacks] for any military or hostile use . . . ."); *see also* Tom Gjelten, *Seeing the Internet as an 'Information Weapon,'* (NPR broadcast Sept. 23, 2010), *available at* http://www.npr.org/templates/story/story.php?storyId=130052701 (asking "why is there no arms control measure that would apply to the use of cyberweapons?"). For a view skeptical that such meaningful agreements can be reached, see Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, *in* FUTURE CHALLENGES IN NATIONAL SECURITY AND LAW, *supra* note 15.

It is not surprising that the United States seems inclined toward an interpretation of Articles 2(4) and 51 that allows it to classify some offensive cyber-attacks as prohibited "force" or an "armed attack" but does not otherwise move previously drawn lines to encompass economic coercion or other means of subversion in that classification. Nor is it surprising to see the United States out in front of other states on this issue. The power and vulnerability distribution that accompanies reliance on networked information technology is not the same as past distributions of military and economic power, and perhaps not to the United States's advantage relative to rivals. Moreover, some U.S. strengths are heavily built on digital interconnectedness and infrastructure that is global, mostly private, and rapidly changing; these strengths are therefore inextricably linked to new and emerging vulnerabilities.[144]

Although some experts assess that the United States is currently strong relative to others in terms of offensive capabilities,[145] several factors make the United States especially vulnerable to cyber-attack, including the informational and electronic interconnectedness of its military and public and private sectors, and political obstacles to curing some of these vulnerabilities through regulation.[146] As the Obama administration's 2010 National Security Strategy acknowledged:

> The very technologies that empower us to lead and create also empower those who would disrupt and destroy. They enable our military superiority . . . . Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale.[147]

In other words, U.S. technological strengths create corresponding exposures to threats.

The U.S. government is especially constrained politically and legally in securing its information infrastructure—which is largely privately held or privately supplied—against cyber-threats, and these constraints shape its international strategy. Proposals to improve cyber-security through regulation include promulgating industry standards to enhance the security of information technology products and protect networks and computers from intrusion, and, more invasively, expanding the government's authority to monitor information systems and communications.[148] Such proposals invariably face powerful antiregulatory industry pressures and heightened civil liberties sensitivities.[149]

---

144. *See* PHILIP BOBBITT, THE SHIELD OF ACHILLES: WAR, PEACE, AND THE COURSE OF HISTORY 792-94 (2002).

145. *See* Jack Goldsmith, *Can We Stop the Global Cyber Arms Race?*, WASH. POST, Feb. 1, 2010, at A17 ("[T]he U.S. government has perhaps the world's most powerful and sophisticated offensive cyberattack capability.").

146. *See* CLARKE & KNAKE, *supra* note 50, at 226-27.

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

148. *See* CLARKE & KNAKE, *supra* note 50, at 160-62; JACK GOLDSMITH, BROOKINGS INST., THE CYBERTHREAT, GOVERNMENT NETWORK OPERATIONS, AND THE FOURTH AMENDMENT (2010), *available at* http://www.brookings.edu/~/media/Files/rc/papers/2010/1208_4th_amendment_goldsmith/1208_4th_amendment_goldsmith.pdf.

149. *See* Lolita C. Baldor, *Internet Security Plan Under Review Would Alert Users to Hacker*

Information technology industry groups and privacy organizations have together pushed back against moves to impose government security mandates and against more intrusive government cyber-security activities, arguing that they would stifle innovation, erode civil liberties, and fail to keep up with rapidly evolving threats amid a globalized economy.[150] A reluctance to secure information systems domestically through government regulation then elevates U.S. government reliance on other elements of a defensive strategy.

In that light, U.S. legal interpretations and declaratory postures that define prohibited force in ways that extend narrow Charter interpretations to take account of cyber-warfare may be seen as part of an effort to sustain a legal order in which anticipated U.S. military and economic moves and countermoves against potential adversaries fit quite comfortably—that is, a legal order that preserves U.S. comparative advantages. In extending the foundational U.N. Charter prohibition on force to cyber-attacks by emphasizing their comparable effects to conventional military attacks, such interpretations help deny that arsenal to others by raising the costs of its use. At the same time, by casting that prohibition and complementary self-defense authority in terms that help justify military force in response, this interpretation reduces the costs to the United States of using or threatening to use its vast military edge (and it helps signal a willingness to do so).

Put another way, the United States appears to be placing hedged bets about what the future strategic environment will look like and how best to position itself to operate and compete in it. On balance, for example, the United States may prefer relatively clear standards with respect to cyber-actions that have immediate destructive effects—at least clear enough to justify armed response or deterrence to activities or scenarios deemed threatening—while at the same time preferring some permissive haziness with respect to intelligence collection and its own countermeasures in cyberspace. Such a posture allows the United States to protect itself from hostile penetrations while also preserving some latitude for those activities in which it may be relatively strong.[151] Internally, that clarity facilitates planning for contingencies and deliberation about options;[152] externally, it may help articulate and deter the crossing of red lines.[153]

In trying to explain what may be driving the U.S. interpretation, this

Takeover, WASH. POST, Oct. 18, 2010, at A17; Nakashima, *supra* note 70. For a discussion on the heavy U.S. reliance on private information infrastructure, see McConnell, *supra* note 5. For a discussion of the intersection of cyber-security and civil liberties, see Gregory T. Nojeim, *Cybersecurity and Freedom on the Internet*, 4 J. NAT'L SEC. L. & POL'Y 119 (2010).

150. In March 2011, for example, industry and civil liberties groups collaborated and published a white paper opposing "government-centric" regulatory approaches to cyber-security. The white paper was published jointly by the Business Software Alliance, Center for Democracy & Technology, U.S. Chamber of Commerce, Internet Security Alliance, and TechAmerica. BUS. SOFTWARE ALLIANCE ET AL., IMPROVING OUR NATION'S CYBERSECURITY THROUGH THE PUBLIC-PRIVATE PARTNERSHIP (Mar. 8, 2011), http://www.cdt.org/files/pdfs/20110308_cbyersec_paper.pdf.

151. *See supra* notes 61-62 and accompanying text.

152. For a discussion of these roles of law, see CHAYES, *supra* note 95, at 88-106.

153. For an overview of deterrence problems in cyberspace, see CTR. FOR STRATEGIC AND INT'L STUDIES, *supra* note 5, at 23-27; and LIBICKI, *supra* note 111, at 39-41.

Article is neither affirming nor denying this strategic logic, which is contingent on future capabilities and vulnerabilities that are both highly uncertain and shrouded in secrecy. Rather, it is trying to uncover and scrutinize some of the underlying assumptions.

There are several strategic reasons for the United States to be cautious in considering interpretations that expand narrow definitions of "force" and "attack" so that they include potentially broad categories of cyber-attacks—risks that are often not acknowledged or addressed in discussions of the U.S. interpretive trajectory. For one thing, the United States has generally defeated efforts by other states to interpret Articles 2(4) and 51 expansively to include economic coercion and other forms of political subversion.[154] In thinking about the Charter regime as a whole, therefore, the United States may not want to reopen those debates. Cyber-attacks can allow state and nonstate actors to inflict massive harm without resort to arms, but that has long been true of many other instruments, including economic and financial means, covert subterfuge, and other widely used instruments. In that regard, one advantage of promoting legal regulation of cyber-attacks through a new treaty or international agreement instead of through Charter interpretation is that such efforts would have little if any effect on broader Charter law. An advantage, however, to working through Charter interpretation rather than new agreements is that Charter law can evolve incrementally and begin shaping international actors' expectations through unilaterally initiated state practice without having to reach consensus (the difficulties of which are discussed in the next Section).

Depending on the relative risk of different types of future cyber-attack scenarios, it might also be in the United States's strategic interest to legally *de-link* cyber-activities from armed force instead of defining force by reference to effects, or at least to impose extremely high legal thresholds for treating cyber-attacks equivalent to force or armed attack, in order to reduce the chances of military escalation from cyber-activities.[155] As capabilities proliferate among state and nonstate actors to conduct various sorts of malicious, hostile, or intelligence-gathering activities in cyberspace, any normative constraints that come from treating some cyber-attacks as force prohibited by Article 2(4) and any deterrence value of treating them as armed attacks triggering self-defense rights under Article 51 might be outweighed by the dangers of lowering legal barriers to military force in a wider range of circumstances.[156] That is, the value

154. *See supra* Section II.A.

155. *See* LIBICKI, *supra* note 111, at 69-70. For a discussion of "low-intensity" cyber-conflict from a strategic and legal standpoint, see Sean Watts, *Low-Intensity Computer Network Attack and Self-Defense*, 87 INT'L L. STUD. (forthcoming 2011), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1685896&.

156. Schmitt argues that a high threshold for self-defense to armed attacks is especially important in the case of cyber-attacks "due to the difficulty states may have in identifying the correct source of an attack." Schmitt, *supra* note 29, at 929; *see also* NRC COMMITTEE REPORT, *supra* note 4, at 256 (discussing costs and benefits to preventing escalation in setting an appropriate threshold for self-defense). Recall from the discussion of the ICJ's *Nicaragua* case that a drawback of a high threshold for self-defense is that it may inadequately deter low-level hostile actions. *See supra* notes 119-121 and accompanying text; *see also* Lewis, *supra* note 43 at 16 ("The development of mutual understandings among nations on thresholds for conflict, including what actions can be considered a violation of

of promoting a right of armed self-defense against cyber-attacks may turn out to be quite low—since, among other things, it may be difficult to sufficiently prove one's case publicly in justifying military responses—while doing so may introduce greater security instability to the international system by eroding normative constraints on military responses to nonmilitary harms.[157]

As the following Section explores, it is very difficult to assess these risk balances because the global security environment is shifting dramatically and unpredictably. Moreover, even if the United States could assess the risks accurately, other states may be operating under different sets of strategic assumptions about that future.

C. *Divergent Interests and Implications for Charter Interpretation*

Assuming the United States decides firmly on a legal interpretation going forward, the redrawing of legal lines on a map of inequitably distributed power and vulnerabilities would create winners and losers and would make it difficult to reach agreement on new legal boundaries, whether through interpretive evolution of the U.N. Charter or new conventions.[158] In thinking about legal interpretations of Articles 2(4) and 51, success therefore depends on the ability of proponents to articulate and defend their legal lines using combinations of traditional and new forms of power for deterrence, self-defense, enforcement, and influence.

Again, one should not divorce analysis of any proposed content of Articles 2(4) and 51 from the processes by which it is interpreted, reinterpreted, enforced, and reinforced.[159] The likely factual ambiguity surrounding cyber-attacks and the pressures to take aggressive responsive or escalatory measures more quickly than those facts can be resolved may sometimes require strategic and military decisionmaking amid legal gray zones. Moreover, as involved states marshal their arguments amid these moves and countermoves, and as they consider their long-term interests, they may also calculate differently what Stone calls "the expected value . . . of built-in [legal] ambiguities as future political weapons."[160]

That is, even if states widely share a common, minimum interest in restricting some cyber-attacks, states may have divergent interests regarding specific substantive content as well as the desired degree of clarity in the law. Salient differences will likely stem from asymmetries of geostrategic ambitions, internal and external commitment to legal norms generally, and the

---

sovereignty, on what constitutes an act of war, and what actions are seen as escalatory, could reduce the potential for cyberwar.").

157. An alternative is to interpret Article 2(4)'s prohibitions of "force" to include some cyber-attacks based on their effects but to interpret Article 51's self-defense "armed attack" trigger narrowly, to exclude cyber-attacks. *Cf.* Schmitt, *supra* note 29, at 928-29 (arguing that if Article 2(4) is interpreted to include cyber-attacks it would be prudent to narrowly interpret states' right to armed self-defense against them).

158. *See* Goldsmith, *supra* note 112, at 26.

159. *See supra* Section III.B.

160. STONE, *supra* note 34, at 242.

nature and extent of public-private institutional relationships.[161]

In contrast to the United States, some states that are developing offensive cyber-warfare capabilities (such as North Korea, according to many experts) are non-status-quo powers or aspiring regional powers,[162] and they may prefer legal ambiguity as to cyber-attacks or narrow interpretations of Article 51 that would allow them—if they resort to cyber-attacks—to portray themselves as victims of any responsive military strikes.[163] Offensive cyber-capabilities have the potential to shift or upset international balances of power, because some states are more vulnerable than others to cyber-attack (in terms of capacity to block actions as well as to tolerate or withstand them), and attacks could have a disproportionately large impact on countries or militaries that have a higher reliance on networked information systems.[164] Developing an offensive cyber-warfare capability is likely to be less expensive in resources and diplomatic costs than competing economically or militarily with much stronger states, though legal flexibility or constraints could alter that calculus.[165] On the other hand, some small states that are unlikely to develop sophisticated offensive or defensive systems may advocate international legal interpretations or new agreements that are very restrictive of cyber-attacks and define attacks broadly,

---

161. *See generally* DANIEL L. BYMAN & MATTHEW C. WAXMAN, THE DYNAMICS OF COERCION: AMERICAN FOREIGN POLICY AND THE LIMITS OF MILITARY MIGHT (2002) (arguing that power relations shape constraints, including legal and diplomatic, under which states can use or threaten force). Internally, some U.S. government officials bristle at what they see as overly restrictive legal constraints. *See* Nakashima, *supra* note 59.

162. *See* Choe Sang-Hun & John Markoff, *Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea*, N.Y. TIMES, July 9, 2009, at A4. Admiral Mike McConnell, the former Director of National Intelligence and Director of the NSA, stated:

> If I were an attacker and I wanted to do strategic damage to the United States, I would either take the cold of winter or the heat of summer, I probably would sack electric power on the U.S. East Coast, maybe the West Coast, and attempt to cause a cascading effect. All of those things are in the art of the possible from a sophisticated attacker.

Quoted in Cyber War: Sabotaging the System, CBS NEWS (Nov. 8, 2009), http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml.

163. Consider, by way of analogy, the *Oil Platforms* case, discussed *supra* notes 77-79 and accompanying text.

164. *See* CLARKE & KNAKE, *supra* note 50, at 259 ("The asymmetry of what it costs to counter our conventional military versus the minimal investment required for a cyber war capability will tempt other nations, and perhaps criminal cartels and terrorist groups as well."); Lynn, *supra* note 5, at 108 ("Cyberattacks offer a means for potential adversaries to overcome overwhelming U.S. advantages in conventional military power and to do so in ways that are instantaneous and exceedingly hard to trace . . . ."); Peter Apps, *Iran "Attack" Points to Rising Cyber Warfare Risk*, REUTERS (Sept. 24, 2010), http://www.reuters.com/article/idUSTRE68N45Q20100924 ("[C]yber warfare is seen as a particularly appealing option for countries that remain far outmatched by the conventional military might of the U.S. North Korea is seen as having particular advantages in any cyber confrontation—its own national computer infrastructure is so outdated that there would be little if anything for South Korea or U.S. cyber warfare experts to counter-attack against."); *see also* U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security: Rep. of the Secretary-General*, at 5, U.N. Doc. A/64/129 (July 8, 2009) (statement of Kazakhstan) (arguing that the lack of consensus on international approaches to regulating cyber-warfare "can be explained by the technological gap between the most and the least develop countries, latent political differences and conflicting ways of assessing developments and events in cyberspace"). For views more skeptical that cyber-capabilities will radically alter power balances, see generally MARTIN C. LIBICKI, CONQUEST IN CYBERSPACE (2007); and GREGORY J. RATTRAY, STRATEGIC WARFARE IN CYBERSPACE (2001).

165. *See* STEWART BAKER, SKATING ON STILTS 218-20 (2010); *see also* U.N. Secretary-General, *supra* note 164, at 3 (statement of Brazil) ("The efficiency of this form of warfare is increased by the fact that relatively small investments are required to develop many of those capabilities.").

seeing themselves as highly reliant on protective norms.[166] Individually, though, they will have little power to promote those principles.

Like the United States, other major actors may have much to lose from cyber-attacks. However, they may calculate their short- and long-term strategic interests with respect to cyber-warfare and its regulation differently than the United States, in light of their own matrix of offensive and defensive capabilities, public-private institutional relationships, and asymmetries in the ways international law constrains different actors.[167] Russia, for example, has proposed to the United Nations a draft statement of principles that would prohibit the development, creation, and use of cyber-attack tools. Meanwhile, though, Russia is engaged in developing cyber-attack capabilities,[168] and some analysts are skeptical of Russia's sincerity in proposing cyber-arms control agreements, especially given the difficulties of verifying them.[169] China likely sees cyber-warfare capabilities as a way of equalizing the conventional military superiority of the United States,[170] so it may be reluctant to concede legally "disarming" interpretations, at least without some reciprocal benefit or legal concession. Russia and China, which, as mentioned earlier, both reportedly exploit informal relationships with private actors (i.e., "citizen hackers") to conduct attacks and collect intelligence in cyberspace, may also incline toward legal doctrine that makes it difficult to impute private cyber-actions to governments.[171] Meanwhile, some European states have approached the legal relationship between cyber-attacks and force cautiously, perhaps because of general concerns about military escalation of crises and divergent strategic assessments among themselves.[172]

Differences in internal politics, ideology, and government control over information will also shape state interests in competing interpretations of

166. *See, e.g.*, U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security: Rep. of the Secretary-General, Addendum*, at 8, U.N. Doc. A/64/129/Add.1 (Sept. 9, 2009) (statement of Mali) ("The use of an information weapon could be interpreted as an act of aggression if the victim State has reasons to believe that the attack was carried out by the armed forces of another State and was aimed at disrupting the operation of military facilities, destroying defensive and economic capacity, or violating the State's sovereignty over a particular territory.").

167. For discussion of such legal jockeying among states, see Sean Kanuck, *Sovereign Discourse on Cyber Conflict Under International Law*, 88 TEX. L. REV. 1571, 1585-87 (2010).

168. *See* NRC COMMITTEE REPORT, *supra* note 4, at 329-32; John Markoff & Andrew E. Kramer, *U.S. and Russia Differ on Treaty for Cyberspace*, N.Y. TIMES, June 28, 2009, at A1.

169. *See* BAKER, *supra* note 165, at 230-31.

170. *See* NRC COMMITTEE REPORT, *supra* note 4, at 332-33; OFFICE OF THE SEC'Y OF DEF., ANNUAL REPORT TO CONGRESS: MILITARY POWER OF THE PEOPLE'S REPUBLIC OF CHINA 27-28 (2009).

171. *See supra* notes 128-129 and accompanying text. For a discussion of doctrine regarding imputing nonstate actors' attacks to a state, see Roscini, *supra* note 29, at 99-102. In more conventional contexts of military attacks, for example, such doctrine sometimes turns on the type and degree of state control or influence over a nonstate actor's actions, but that doctrine is difficult to apply in the cyber-context because conventional military operations usually involve stricter hierarchical control and other indicia (like provision of military materiel) than one might expect here. *See id.*

172. *See supra* note 57 (discussing NATO's tentativeness). In light of Estonia's experience, however, some European states may take a more aggressive view, closer to that of the United States, and place a greater value on deterrence. *See* Kodar, *supra* note 49, at 139 (discussing the Estonian perspective).

Charter norms. With echoes of debates from prior eras,[173] various types of states are likely to view cyber-threats differently and to distinguish offensive attacks from defensive measures differently. For instance, some states that tightly control information, including major powers like China, are especially concerned about internal political dissent and might therefore define what the United States sees as "Internet freedom" as a threat to vital security interests. Efforts to crack down on what they (or other states that exercise strong state control over Internet content) may view as defensive measures against hostile subversion may be viewed by the United States (or other states that value and promote free speech) as hostile, offensive measures.[174] It is hard to envision a state in China's position strongly endorsing or standing behind U.S. visions for international legal regulation of cyber-attacks without some unlikely concessions by the United States.[175]

From a policy standpoint, this should sound another cautionary note about efforts to build international legal consensus about cyber-attacks and the use of force, whether through Charter interpretation or new agreements. Emergent U.S. government inclinations toward effects-based interpretations of the Charter may be legally reasonable and protective of some core U.S. interests, as well as widely shared foreign interests. But even if they help in the short term to manage competing risks of too much or too little authority to employ cyber-attacks, or too much or too little leeway to resort to armed self-defense in response, a coherent legal strategy can only be forged and advanced in the long term if it is integrated effectively with broader diplomacy and security strategy, including efforts to build and sustain offensive, defensive, deterrent, and intelligence capabilities—while others do the same based on a different set of objectives, capabilities, vulnerabilities, and constraints.

* * *

173. As an example of such echoes, a Russian representative to a 2008 U.N. disarmament conference revived old Soviet arguments about "ideological aggression," arguing that efforts to promote ideas on the Internet in order to subvert another country's government should qualify as aggression. *See* Gjelten, *supra* note 143; *cf.* Franck, *supra* note 87, at 814 ("[O]ne has only to have experienced a revolution in Africa or the Middle East to know that an effective, radio transmitter may be worth more than its weight in grenades and pistols.").

174. In the same address quoted earlier in which Secretary of State Clinton spoke of defending against attacks on U.S. networks or information flow, she went on to discuss U.S. efforts to help political dissidents evade state Internet censorship and to promote political change via Internet freedom in repressive states, including technical support. *See* Clinton, *supra* note 55; *see also* Goldsmith, *supra* note 143 (discussing this policy tension).

A set of 2010 incidents involving Google and China is illustrative. Google alleged that its systems had been penetrated, resulting in the surveillance of and crackdown on Chinese political activists. The United States responded diplomatically in ways suggesting that the Chinese government had launched this hostile assault on Google's systems. *See* Michael Wines, *China Issues Sharp Rebuke to U.S. Calls for an Investigation on Google Attacks*, N.Y. TIMES, Jan. 26, 2010, at A6. Although China denied involvement, it likely viewed any such actions as defensive against subversive efforts being waged over those systems. *Id.*; *see also* Eric Schmidt & Jared Cohen, *The Digital Disruption: Connectivity and the Diffusion of Power*, FOREIGN AFF., Nov./Dec. 2010, at 75, 76 ("There will be a constant struggle between those striving to promote what U.S. Secretary of State Hillary Clinton has called 'the freedom to connect' and those who view that freedom as inimical to their political survival.").

175. *See* Goldsmith, *supra* note 143, at 7-9.

As the opening U.S.-Iran hypothetical as well as early Cold War legal debates demonstrate, the policy imperative to align legal moves with broader strategy has long existed with respect to other inequitably distributed forms of strength and vulnerability, including military might, economic prowess, and surreptitious political influence. Since the Charter's creation, the United States, like its partners and rivals, has pursued an international legal strategy in the context of grand geopolitics, resulting in a dynamic interplay of law and power: states' instruments for exerting power and their vulnerabilities to them shape their approaches to legal interpretation, while legal constraints in turn affect the instruments of statecraft and vulnerabilities.

The same policy imperatives hold with respect to the United States's ability to compete in an emergent cyber-security environment likely to include powerful actors with divergent interests and those who would violate whatever legal lines begin to emerge,[176] and a world in which rapidly developing technology will reshape the nature and distribution of power.[177] The prescription is not to abandon interpretive or multilateral legal efforts to regulate cyber-attacks, but to recognize their likely limits and to consider the implications of legal proposals or negotiations in the context of a future security environment that is shifting radically and fraught with uncertainties.

V. CONCLUSION

Cyber-attacks pose difficult line-drawing problems, but we must avoid missing the strategic forest in thinking about the legal trees. Some problems of cyber-warfare for regulating force are at the same time unique yet familiar. Viewing these questions in the context of Cold War debates about the U.N. Charter and its prohibition of "force" highlights that although the technology of conflict—both in terms of capabilities and probable vulnerabilities—is changing in revolutionary ways, many of the interrelated strategic and legal challenges that arise are not new.

Legal line drawing with respect to the U.N. Charter and use of force norms creates geostrategic winners and losers, so debates about Charter interpretation have always reflected distributions of power and vulnerability. That lesson helps to explain what appears to be the emergent—though not yet formalized and publicized—U.S. legal orientation on cyber-attacks, as well as some of the nascent re-posturing from the standard American stance on the use of force through much of the Charter's history.

Even if the U.S. government's assumptions about threats and conflict bear out in an uncertain future, other major state actors in this area are likely to have different views on legal line drawing because they perceive a different set

176. *See* NRC COMMITTEE REPORT, *supra* note 4, at 69-70.

177. *See* Anne-Marie Slaughter, *America's Edge: Power in the Networked Century*, FOREIGN AFF., Jan./Feb. 2009, at 94; *see also* Schmidt & Cohen, *supra* note 174, at 75 ("For the world's most powerful states, the rise of the interconnected estate will create new opportunities for growth and development. . . . States will vie to control the impact of technologies on their political and economic power.").

of strategic risks and opportunities. It will therefore be difficult to reach interpretive agreement. Moreover, particular characteristics of cyber-attacks—including the low visibility of attacks and counter-actions, likely disputes about key facts, and difficulties in establishing attribution and causation—will make it especially difficult to build legal consensus around the U.S. position. For the foreseeable future, the United States will have to pursue its offensive and defensive strategy on an uncertain and unstable international legal terrain.