Navigating Conflicts in Cyberspace: Legal Lessons from the History of War at Sea

Jeremy Rabkin
Ariel Rabkin

Follow this and additional works at: https://chicagounbound.uchicago.edu/cjil

Part of the Law Commons

Recommended Citation
Available at: https://chicagounbound.uchicago.edu/cjil/vol14/iss1/7

This Article is brought to you for free and open access by Chicago Unbound. It has been accepted for inclusion in Chicago Journal of International Law by an authorized editor of Chicago Unbound. For more information, please contact unbound@law.uchicago.edu.
Navigating Conflicts in Cyberspace: Legal Lessons from the History of War at Sea
Jeremy Rabkin* and Ariel Rabkin†

Abstract

Despite mounting concern about cyber attacks, the United States has been hesitant to embrace retaliatory cyber strikes in its overall defense strategy. Part of the hesitation seems to reflect concerns about limits imposed by the law of armed conflict. But analysts who invoke today’s law of armed conflict forget that war on the seas has always followed different rules. The historic practice of naval war is a much better guide to reasonable tactics and necessary limits for conflict in cyberspace. Cyber conflict should be open—as naval war has been—to hostile measures short of war, to attacks on enemy commerce, to contributions from private auxiliaries. To keep such measures within safe bounds, we should consider special legal constraints, analogous to those traditionally enforced by prize courts.

Table of Contents

I. Introduction ................................................................. 198
II. Offensive Operations At Sea: An Overview.......................... 202
III. Arming Merchant Ships and Other Instructive Analogies ......... 212
IV. Jus Ad Bellum. When Cyber Retaliation is Justified............... 220
V. Permissible Targets and the Problem of Attribution................... 231
VI. Who Are Lawful Combatants in Cyberspace? ...................... 239

* Professor of Law, George Mason University; PhD, Political Science, Harvard University.
† Post-Doctoral Researcher, Department of Computer Science, Princeton University; PhD, Computer Science, University of California, Berkeley. The authors thank Ken Anderson, Stewart Baker, Gabriella Blum, Philip Bobbitt, Jack Goldsmith, Abram Shulsky, Matthew Waxman and John Yoo for comments on an earlier version of this article and also thank Chris Grier and Vern Paxson for their advice on legal issues facing researchers in the field of computer security. The authors also thank Rachel Parker of the George Mason University School of Law for energetic and astute research assistance.
In the summer of 2011, General James E. Cartwright, the vice chairman of the Joint Chiefs of Staff, expressed frustration with the government's current approach to cyber attacks: "If it's OK to attack me, and I'm not going to do anything other than improve my defenses every time you attack me, it's very difficult to come up with a deterrent strategy." At the time, there was much dispute about whether the United States could use cyber technology as an offensive weapon and, if so, in what circumstances.

A few weeks later, the House of Representatives sought to clarify the issue with a provision in the 2012 Defense Authorization Act: "Congress affirms that the Department of Defense has the capability, and, upon direction by the President, may conduct offensive operations in cyberspace to defend our Nation, Allies and interests." The Senate insisted on a qualification, however, which was duly inserted in the final text of the legislation: "subject to—(1) the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict; and (2) the War Powers Resolution."
In June of 2012, The New York Times published a detailed account of an elaborate, long-term American effort to disrupt Iran’s nuclear weapons program.\(^5\) A customized computer virus, Stuxnet, devised by American programmers, had been introduced into the equipment regulating Iranian centrifuges, causing the centrifuges to malfunction, thereby setting back Iranian efforts to purify uranium to the level required for nuclear weapons. The disclosure of the American effort provoked an uproar—\(^6\) but only about whether the Obama administration had been negligent in protecting American military secrets or had engaged in deliberate, self-serving leaks to portray itself as “tough” on national security.\(^7\) The White House offered no explanation of why the cyber attack on Iranian facilities was consistent with “the law of armed conflict.” Congress did not demand any explanation.

Many legal questions might have been raised, since Iran had not yet achieved a workable nuclear device, let alone entered into a confrontation in which its use could be seen as “imminent.” The Iranian government insisted that its uranium purification plants were for “civilian” rather than “military” purposes. Most commentators on the “law of armed conflict” insist that it prohibits “attacks” on “civilian objects.” There was almost no public debate, however, on whether the American cyber sabotage program was consistent with “the law of armed conflict”—let alone with the War Powers Resolution, requiring notification of Congress before resorting to military action.

---

\(^5\) David Sanger, Obama Order Sped Up Wave of Cyberattacks Against Iran, NY Times A1 (June 1, 2012).


\(^7\) Steve Bucci, Stuxnet Revelation Continues Obama Administration Trend of Classified Leaks, The Foundry (June 1, 2012).
In September of 2012, the Legal Adviser to the State Department, Harold Koh, spoke at an inter-agency conference hosted by US Cyber Command.\(^8\) He affirmed that cyber attacks which caused "death, injury or significant destruction would likely be viewed as a use of force," triggering the right to exercise force in self-defense, as authorized by the UN Charter. He also insisted that, "As in any form of armed conflict, the principle of distinction requires that the intended effect of the attack must be to harm a legitimate military target." He did not explain how or why the Iranian nuclear program was a "legitimate military target." He did not speculate on whether Iran might be entitled to retaliate for US attacks. Most tellingly, Koh did not make any effort to explain what sorts of cyber retaliation the United States might feel entitled to undertake, should persistent and costly cyber attacks fall below the threshold of destructiveness associated with an "armed attack."

But US government officials have acknowledged that American facilities—both military and civilian, both government and private—are continually subject to probing, spying, and disrupting attacks from foreign entities, some clearly sponsored by powerful foreign states.\(^9\) That was the context of General Cartwright’s expression of concern about whether the United States can hope to defend against foreign cyber attacks if it never retaliates. Neither General Cartwright nor any other American official has offered any public clarification of when, how, and under what rules the United States might retaliate against cyber attacks. In the spring of 2013, the Obama administration did voice public protest over Chinese cyber theft of American trade secrets. It failed to make any threat of retaliation, however, calling instead for "dialogue to establish norms of behavior in cyberspace."

Official policy seems to regard cyber weapons as subject to the law of armed conflict but actual practice remains quite murky and obscure. Evidently, the hesitation to clarify American policy reflects enduring concerns about international legal standards. Some months before Koh’s address, Stewart Baker,

\(^8\) Harold Hongju Koh, Remarks at USCYBERCOM Inter-Agency Legal Conference (Sept 18, 2012), transcript available online at http://www.state.gov/s/l/releases/remarks/197924.htm (visited Mar 1, 2013).


former General Counsel to the National Security Agency (NSA) (and former Assistant Secretary for Policy at the Department of Homeland Security), protested that government lawyers were "tying themselves in knots of legalese . . . to prevent the Pentagon from launching cyber attacks."11

While US officials may have doubts, the International Committee of the Red Cross (ICRC) does not. It insists that the law of armed conflict does apply to cyber conflict. According to the ICRC, the rules set out in the most recent and most comprehensive treaty on this subject, Additional Protocol I (AP I) to the Geneva Conventions (1977), apply in full to cyber conflict.12 A similar view has been elaborated in The Tallinn Manual on International Law Applicable to Cyber Warfare, prepared by an "international group of experts" advising the Cyber Defence Centre of the North Atlantic Treaty Organization (NATO).13 A long line of commentators embraces much the same view.14

But these commentators reach this conclusion by a chain of reasoning that seems rather Pickwickian. They start, almost invariably, with general treaties and respectable treatises on the law of armed conflict, usually following the lead of earlier Red Cross commentaries. Commentators proceed by delving into current literature on cyber threats. Then, like the critic for the provincial Eatonsville Gazette, whose work was touted to Mr. Pickwick, they have simply "combined [their] information."15

We do not argue that cyberspace should be regarded as a law-free zone. We emphatically do not argue that cyber attacks can be deployed without any


15 Dickens, The Pickwick Papers at 646 (cited in note 1).
regard to legal limits on their effects. Instead, we argue that it would be more appropriate to ground American policy on cyber attacks in an older and in some ways better established body of law and practice—that dealing with armed conflict on the high seas. There was always a considerable body of law regulating armed conflict at sea but it was not the same law as that applied to land warfare—let alone the more ambitious rules of armed conflict advocated in recent decades by the International Red Cross.

In the next section, we offer a general survey of ways in which war at sea embraced different legal restraints—and why these historic limitations might seem more applicable to contemporary cyber conflict than what the Red Cross calls "International Humanitarian Law." In Section III, we elaborate on analogies to particular defensive practices embraced by Britain and the United States in the world wars of the twentieth century. In Section IV, we apply naval practice to questions about when it is proper to resort to force if the relevant "force" is a cyber attack. In Section V, we apply these analogies to analyze proper targets in cyberspace and in Section VI, proper participants. Section VII looks at ways to reassure third parties about legal restraints on cyber attacks, building on the analogy with prize courts and other established practices in other fields of unconventional conflict. Section VIII offers some concluding thoughts about the prospects for building a customary law of cyber conflict, analogous to the historic practice in conflict on the seas.

II. OFFENSIVE OPERATIONS AT SEA: AN OVERVIEW

War at sea bears obvious comparison with cyber conflict. A number of commentators have already noticed parallels in the setting, though without drawing out the full implications.¹⁶ Like the high seas, the cyber realm is not confined within the territory of individual states. Like the high seas, it has become a vital pathway of commerce and communication. The special challenge of naval war was to prevent conflicts between belligerents from interfering with legitimate neutral shipping. Cyber conflict raises analogous concerns about cyber disruptions affecting third parties.

A central aim in the law of war on land was to confine war to combatants, often called the principle of "distinction." That is the main principle stressed by the International Red Cross when it admonishes that cyber conflict must respect the "law of armed conflict." As the Red Cross emphasizes in its commentaries on treaty law in this area, the principle of distinction can be traced back many

---

centuries—even if (as the Red Cross fails to acknowledge) there were always exceptions in law and more so in practice.\textsuperscript{17}

The background impulse is often described as “humanitarian”—seeking to avoid unnecessary suffering, particularly to innocents. But such abstract appeals for “humanity” cannot be directly equated with the legal standard of “distinction.”\textsuperscript{18} In war on land, there were also practical reasons to respect the more specialized rule of “distinction.” The usual object in land warfare was to seize and hold enemy territory. For an invading army, it was often helpful to promise immunity to civilians in the newly seized territory in order to promote civilian cooperation with the ensuing occupation.

The first thing to notice about the historic law of war at sea is that it followed its own rules. In contrast to the developing trend in land warfare by the

\textsuperscript{17} Red Cross commentators insist that the principle of “distinction”—between permissible military targets and unlawful civilian targets—is “the foundation on which the codification of the laws and customs of war rests.” Claude Pilloud, et al, \textit{Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949} 598 (Martinus Nijhoff 1987). The earliest source cited in support of this claim is the 1868 “St. Petersburg Declaration” which stipulated “the only legitimate objective which States endeavor to accomplish during war is to weaken the military forces of the enemy.” \textit{Declaration Renouncing the Use, In Time of War, of Explosive Projectiles under 400 Grammes Weight} (1868), online at http://www.icrc.org/ihl.nsf/FULL/130?OpenDocument (visited Apr 9, 2013). But as even the Commentary acknowledges, this admonition was “concerned with preventing superfluous injury or unnecessary suffering to combatants” (emphasis added)—the “Declaration” sought to prohibit use of explosive bullets against soldiers in battle—“and was not aimed at specifically protecting the civilian population.” It was not until Additional Protocol I, completed in 1977, that a convention on the law of armed conflict included anything approaching a total prohibition on attacks directed at civilian property. Horace B. Robertson, Jr, \textit{The Principle of the Military Objective in the Law of Armed Conflict}, 72 \textit{Int'l Law} Studies 197, 197 (1998).

\textsuperscript{18} See, for example, Gary Solis, \textit{The Law Of Armed Conflict} 250–57, 269–71 (Cambridge 2010) (sets out “distinction” as one of “four core principles” in its overview, then discusses avoiding “unnecessary suffering” as a separate “core principle”). See similarly, Geoffrey S. Corn, et al, \textit{The Law Of Armed Conflict: An Operational Approach} 115–24 (Wolters Kluwer 2011) (identifies “Military Necessity” and “Humanity” as “Cardinal Principles,” then discusses “Distinction” and “Proportionality” as “Implementation Principles”). The Hague Convention on Laws and Customs of War on Land, the classic early source, prohibited signatories to “employ arms, projectiles or material calculated to cause unnecessary suffering” without limiting the prohibition to weapons affecting civilians. \textit{Laws and Customs of War on Land} ( Hague IV), Annex: Art 23(e), 36 \textit{Stat} 2277, 187 \textit{CITS} 227 (1907). That convention did not even use the term “civilian” (except in one provision—Annex: Art 29—dealing with “soldiers and civilians . . . entrusted with the delivery of despatches [sic],” which specified that such adjuncts to military operations were not to be treated as “spies”). Treatises urging constraints on warfare appeared as long ago as the sixteenth century but the \textit{Oxford English Dictionary} records no use of the term “civilian”—in the sense of non-military—until the late eighteenth century and no use of derivative terms such as “civilian casualty” or “civilian target” (terms seemingly so relevant to modern discussions of “humanitarian law”) before the twentieth century. \textit{Oxford English Dictionary} (Oxford 3d ed 2013), online at http://www.oed.com/view/Entry/33577?redirectedFrom=civilian& (visited Apr 16, 2013).
eighteenth century, naval war never exempted civilian property from attack.\textsuperscript{19} To the contrary, disrupting enemy commerce was always a main objective for war at sea and remained so through the twentieth century. The concern was not to spare civilian property, per se, but to avoid provoking bystanders.\textsuperscript{20}

Every major maritime power, starting as far back as the late Middle Ages, established prize courts, where owners of seized ships (or their cargoes) could contest such seizures. While enemy shipping was regarded as lawful prize of war, owners of neutral ships (or neutral cargoes) claimed exemptions from belligerent seizures. Prize courts tried to work out doctrines balancing accepted war measures against reasonable neutral complaints. And it was worthwhile for national prize courts to try to accommodate neutral claims in order to keep neutrals from joining with avowed enemies in open war against the seizing state.\textsuperscript{21}

The provision in the US Constitution, authorizing Congress to issue "Letters of Marque and Reprisal,"\textsuperscript{22} reflects the traditional practice of targeting enemy commerce. Letters of marque could increase the naval capacity of a country with few actual warships. They authorized captains of private ships to attack enemy commerce with the promise that they could keep some of the spoils as reward for their effort.\textsuperscript{23} Suitably refitted with naval guns, a fast-moving merchant ship might hope to seize an enemy merchant ship. It could not expect to prevail in a direct engagement with an enemy warship, which would usually have more and more powerful guns.

Sea raiders with letters of marque acted much like pirates. More than a few had learned their craft as actual pirates.\textsuperscript{24} Pirates did not engage warships when they could avoid doing so. They sought to steal cargoes from merchant vessels. What the letter of marque offered was an assurance that the holder would not

\textsuperscript{19} See generally Donald A. Petrie, \textit{The Prize Game: Lawful Looting on the High Seas in the Days of Fighting Sail} (Naval Institute 1999).

\textsuperscript{20} For historical overview, see John Hattendorf, \textit{Maritime Conflict} in Michael Howard, George J. Andreopoulos, and Mark R. Shulman, eds, \textit{The Laws Of War: Constraints On Warfare In The Western World 103-13} (Yale 1994).

\textsuperscript{21} For an account of prize court procedure and the effects of such rulings on neutral commerce during the seventeenth and eighteenth centuries, see Philip Jessup and Francis Deak, \textit{1 Neutrality, Its History, Economics and Law} 201-60 (Octagon 1976) (concluding that "neutrality was abandoned in favor of belligerency" when "political or commercial self-interest pointed in another direction.")

\textsuperscript{22} US Const Art 1, § 8, cl 11.

\textsuperscript{23} See Hattendorf, \textit{Maritime Conflict} at 103-13 (cited in note 20).

\textsuperscript{24} William C. Davis, \textit{The Pirates Lafitte: The Treacherous World of the Corsairs of the Gulf} 28–29 (Harcourt 2005) (describes the buccaneering background of adventurers who assisted General Jackson at the Battle of New Orleans and then received letters of marque from the US government to prey on Spanish commerce).
attack indiscriminately—that is, would not molest neutral traffic. That commitment obligated neutrals to leave the authorized raider alone. It obligated enemy warships to treat the authorized raider as an enemy prisoner rather than a criminal, since the raider was doing nothing but what a warship might do, under accepted naval tactics.25

Letters of marque, still an important part of US naval strategy in the War of 1812, were disavowed by European powers in the peace settlement after the Crimean War. At the time, the United States refused to endorse the 1856 Declaration of Paris. Instead it urged a more comprehensive ban on all attacks against private property at sea. A number of European states also urged such a general prohibition, which would have brought naval war into line with emerging norms of land warfare.

But no such general prohibition was accepted. Part of the reason was that Britain, with the world’s largest merchant fleet in the nineteenth century, also had the world’s largest navy. Britain did not want to forego the benefits of deploying the full capacities of its navy in wartime merely to protect civilian shipping—which might be well protected by the Royal Navy in any case.26 Commentators in the early twentieth century noted that as other powers built formidable navies, they also came to resist restrictions on naval warfare.27

If we think about the potential of cyber attacks to disable targets from a great distance, cyber conflict must appear, at the outset, much more like classic naval warfare. There is no need to secure cooperation from civilians in the target state. Cyber attacks do not depend on seizing or holding any particular territory.

A government conducting cyber attacks would not, of course, be exempt from the general principle of “humanity,” requiring military action to limit


26 Lassa Oppenheim, 2 International Law § 178 at 222 (Longmans 2d ed 1912) notes:

[T]he abolition of the rule [allowing capture of enemy merchant ships in wartime] would involve a certain amount of danger to a country like Great Britain whose position and power depend chiefly upon her navy. The possibility of annihilating an enemy’s commerce by annihilating his merchant fleet is a powerful weapon in the hands of a great naval Power.

27 Oppenheim, International Law further notes:

Since the growth of navies among continental Powers, these Powers have learnt to appreciate the value of the rule [allowing capture of enemy merchant ships] in war, and the outcry against capture of merchantmen has become less loud. [Today], it may perhaps be said that, even if Great Britain were to propose the abolition of the rule, it is probable that a greater number of the maritime States would refuse to accede. For it should be noted that at the Second [Hague] Peace Conference, France, Russia, Japan, Spain, Portugal, Mexico, Colombia, and Panama, besides Great Britain, voted against the abolition of the rule.

Id at 223.
suffering or harm to the extent feasible. The law of war has recognized claims of “humanity” even when it declined to confer blanket immunities for civilians and civilian property. Historically, war on the seas was war on enemy commerce and private property belonging to enemy nationals. But it was not intended to be a generalized slaughter.

In the eighteenth and nineteenth centuries, commerce raiders would typically place some of their own crew on a seized merchant ship, then sail the whole ship, with all its own crew and cargo, to a home port of the raiding state. Where the raiders could not spare enough of their own crew members to man the seized ship, they might sink it—but only after taking the seized crew to safety. There remained a common interest in protecting fellow mariners against ocean perils, the so-called “fellowship of the sea.”

These restraints broke down in the world wars of the twentieth century—a reminder that the destructive capacity of new technologies is not easily contained, at least in a long war. The next section will discuss the particular challenges raised by submarine warfare during the world wars. For present purposes, it is most pertinent to notice that established constraints were abandoned or severely eroded in several areas, even by the Western Allies. In post-war efforts to re-establish limiting rules, however, the United States and other western nations insisted on reserving their rights to exercise wider tactics in war at sea.

During the Second World War, Britain and the United States engaged in bombing of cities on an unprecedented and frightening scale. The Germans and Japanese had started this practice in their initial aggressions. The Allies

28 See note 18. As another example, consider the Lieber Code, adopted by the Union army during the American Civil War, which was so much of a milestone in the development of the law of armed conflict that the International Red Cross still includes it on its website offering of historic documents in international humanitarian law. Instructions for the Government of Armies of the United States in the Field (Lieber Code) (1863), online at http://www.icrc.org/ihl.nsf/INTRO/110?OpenDocument (visited Apr 16, 2013). The Code prohibits “the wanton devastation of a district” and admonishes that “the unarmed citizen is to be spared in person, property, and honor as much as the exigencies of war will admit.” Id at Art 16, 22. It nonetheless approves “all destruction of property and obstruction of the ways and channels of traffic, travel or communication” and holds it “lawful to starve the hostile belligerent, armed or unarmed, so that it leads to the speedier subjection of the enemy.” Id at Arts 15, 17.


30 For a recent sympathetic analysis of the Allied strategic bombing campaign, see Michael Burleigh, Moral Combat, Good and Evil in World War II, 478–506 (HarperCollins 2011) (explaining rationale for Royal Air Force slogan that forms chapter title: “‘The King’s Thunderbolts Are Righteous’”).

31 Andrew Roberts, The Storm of War, A New History of the Second World War (HarperCollins 2011) (effects of German bombing of Warsaw in September 1939 at 21–22) (effects of German bombing of Rotterdam in May 1940 at 58) (effects of German bombing of London and other
perfected and intensified it, causing hundreds of thousands of civilian casualties and vast physical destruction. At the war crimes tribunals convened in Nuremberg and Tokyo in 1945, no one was charged with violating the laws of war by engaging in indiscriminate air attacks.32 Allied governments did not want to challenge the legality of practices they had themselves adopted.33 There were no general restraints on targeting in the four Geneva Conventions negotiated in 1949.34

It was not until the mid-1970s that an international conference was prepared to assert serious new constraints on the conduct of military operations. The resulting treaty, Additional Protocol I (AP I) to the Geneva Conventions emerged from the first conference on this topic dominated by Third World countries.35 The fate of that treaty suggests the difficulty of imposing new limitations by majority vote of all nations. The United States ultimately refused to ratify the convention. A number of regional powers—Turkey, Iran, Israel, India, Indonesia among others—also declined to ratify AP I. Leading states in the North Atlantic Treaty Organization, including Britain, Canada, Germany, and Italy, ratified only with important reservations. Among other things, their reservations declined to embrace AP I provisions which prohibit reprisals in kind against enemies that engage in unlawful targeting.36

---

33 Id.
34 Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention), 75 UNTS 31 (1949) (providing protections for "wounded and sick" combatants and medical personnel); Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (Second Geneva Convention), 75 UNTS 85 (1949) (providing parallel protections for "wounded, sick and shipwrecked" combatants at sea); Geneva Convention relative to the Treatment of Prisoners of War (Third Geneva Convention), 75 UNTS 135 (1950) (setting out protections for "prisoners of war" in enemy captivity); Geneva Convention relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention), 75 UNTS 287 (1950) (the only Geneva Convention to cover protections for "civilians"—but it limits its protection to persons already "in the hands of" enemy forces or under an "occupying power," so it is not relevant to targeting across battle lines in the midst of an active conflict).
35 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) 1125 UNTS 3 (1977) (extending protections to colonial disputes, alien occupations, and racist regimes).
Almost all the limiting provisions in AP I did find their way into the Statute of the International Criminal Court (ICC), negotiated in 1998. Again, however, the United States and a considerable number of other powers (including Russia, China, India, Pakistan, Israel, Egypt, Indonesia) have declined to ratify the ICC Statute. The court’s actual authority remains somewhat in doubt, having completed only one trial in its first decade in operation. Conflicts in recent decades have not often displayed close adherence to AP I standards.

Whatever one thinks of these developments, it remains notable that major naval powers—including a number of formal signatories to AP I—have declined to embrace AP I as a guide to permissible tactics in war at sea. Naval powers have made no effort to draw the rest of the world into bargaining on how they might lawfully use their sea power in time of conflict. Instead, officials and experts from western naval powers conducted informal discussions, leading to the publication of the 1994 San Remo Manual, which purports to summarize the understanding of experts “on international law applicable to armed conflicts at sea.” It is not a binding convention, but it is the most comprehensive statement of what specialists from leading naval powers regard as applicable customary law.

The San Remo Manual acknowledges that nations in today’s world must hold themselves to higher humanitarian standards than those displayed by Allied navies in the world wars. The Manual accordingly emphasizes a responsibility

allowed to enforce contemplated limits). The Tallinn Manual acknowledges that a number of NATO nations, “notably” Britain and France, are not bound by AP I prohibitions on reprisals, nor are non-signatories and disputes the claim that prohibitions on reprisals have now become a binding rule of customary international humanitarian law. See Rule 47, Reprisals Under AP I, in Schmitt, The Tallinn Manual at 126–27 (cited in note 13).

37 See Ratification/Accession and Signature of the Agreement on the Privileges and Immunities of the Court (APIC) by Region, ICC Fact Sheet, online at http://www.iccnow.org/documents/CICC_APIList_current.pdf (visited Apr 11, 2013) (excluding the US, Russian, China, India, Pakistan, Israel, Egypt, and Indonesia from the list of countries that have ratified).


39 Charles J. Dunlap, Jr., The End of Innocence: Rethinking Noncombatancy in the Post-Kosovo Era, Strategic Rev 9, 16 (2000). (“Even the most ardent zealots of [the Law of Armed Conflict] admit its rules are often unknown, or if known, ignored. A cursory review of the savage conflicts of the last twenty years in the Balkans, Sudan, Lebanon, Sierra Leone, Chechnya, Sri Lanka and elsewhere proves that lamentable point.”)

40 The conference was convened by the International Institute of Humanitarian Law, located in San Remo, Italy. Louise Doswald-Beck, ed, San Remo Manual on International Law Applicable to Armed Conflicts at Sea 5 (Cambridge 1995).

41 Id.

42 Id at 7, ¶¶ 1, 2.
to avoid direct injury to civilians at sea and to avoid blockade measures imposing starvation or extreme privation of civilians on land. But it does not otherwise prohibit attacks on enemy commerce at sea. It specifically provides for seizure of enemy merchant ships to prevent a wide-range of cargo from going in or out of enemy ports. It also authorizes seizure of cargo from neutral ships when the contents may be susceptible for use in armed conflict.

The San Remo Manual thus offers a much more encompassing approach to permissible targets than that proclaimed in AP I. The latter treaty limits attacks to objects "whose total or partial destruction ... in the circumstances ruling at the time, offers a definite military advantage." AP I, which never mentions conflict at sea, seems to be concerned with attacks on "objects" situated in enemy territory—on land. Such "objects" would normally be attacked from a distance—by air strikes or artillery—so the effectual choice would often be between "total or partial destruction" of such "objects," on the one hand, or their total exemption from targeting, on the other.

The San Remo Manual focuses on interventions at sea, where the target vessel might be seized by naval warships and diverted into homeports of the attacking navy, without loss of life and perhaps without any physical destruction. The opportunities offered by intervention on the seas encourage a much more permissive approach. Major naval powers, certainly western powers, seem determined to maintain that range of permissiveness. They do not deny the claims of humanitarian restraint but interpret these claims in more qualified terms.

Here again, there are clear analogies with cyber conflict. Millions of hackers around the world can hope to achieve some damage to targets, temporarily disrupting service. Such attacks are immediately detectable and can, in most cases, be repaired rather quickly. Only a few governments have invested in major research and support efforts for sustained infiltration of targets in ways that are not easily detected and not easily repaired. That is what made the Stuxnet attack on the Iranian nuclear program so remarkable—that it continued to

43 Id at 179, ¶ 102
44 Doswald-Beck, San Remo Manual at 146–51, ¶ 60(g) (cited in note 40).
45 Id at 215–16 ¶ 148.
47 Doswald-Beck, San Remo Manual at 5 (cited in note 40) (most of AP I "is only applicable to naval operations which affect civilians and civilian objects on land").
disable Iranian centrifuges while concealing its operation from Iranian technicians, by sending false signals to monitoring equipment. That sort of “attack” requires far too much sophistication to be improvised by amateur hackers. 49

As major naval powers have claimed wider powers in war at sea, similar latitude will likely be claimed (or exercised) by those states that are most active in the new field of cyber conflict. The most serious challenges will arise from states that can sustain heavy investments to develop and deploy the most advanced means of attack. Probably fewer than a dozen states have the financial resources, the requisite base of technical capacity, and the military commitment to compete in this field. We should not expect agreement among these powers on limiting their capacities, especially if they must negotiate such limits with vast numbers of bystanders, as has now become the accepted practice regarding treaties on the law of armed conflict. Less formal understandings, like the San Remo Manual, might have more promise.

Still, the capacity to impose harm at lower levels is quite pervasive in the cyber realm—just as it was for ocean commerce when pirates stalked the seas (as they still do in some regions, now joined by terrorists). Pirates and terrorists do not need submarines and aircraft carriers to impose serious costs on seaborne commerce. Criminal gangs engage in hacking efforts to steal secrets, scam the gullible, and extort protection payments from the vulnerable. As with pirates in earlier times 50 and terrorists today, much cyber crime has the tacit support of governments. Even when it comes to crime control—or operations on the boundaries between crime control and armed conflict—the law and practice of naval power offers instructive analogies for cyber conflict.

The UN Convention on the Law of the Sea (1982) insists that the “high seas shall be reserved for peaceful purposes” 51 and limits the authority of warships to interfere with foreign shipping to a narrow set of circumstances,

---

49 The success of this particular strike seems to have depended on close cooperation from Siemens, the German industrial firm that supplied equipment to the Iranian program. Not every attacker could expect to receive such assistance from a western manufacturer. Benjamin Weinthal, Iran Accuses Siemens of Sabotaging Nuclear Program: German Company Denies Claims by Iranian Lawmaker, Who Says It Sold Iran Nuclear-Related Equipment Embedded With Small Explosives, Jerusalem Post 2 (Sept 23, 2012).

50 Jennifer Marx, Pirates and Privateers of the Caribbean 26 (Krieger 1992) (describing the British government’s connivance at attacks on Spanish commerce from the time of Francis Drake in the sixteenth century until well into the eighteenth century, characterizing efforts to suppress unlicensed—that is, entirely piratical—attacks as “uneven at best, intensifying or not according to the questions of politics and economics” of the moment).

apart from actual military operations in wartime. Still, the treaty includes a half
dozzen separate provisions concerned with apprehension of pirates on the seas.
Ships suspected of involvement in piracy may be stopped and boarded by
warships of any nation. There is no generally recognized right for a state with
mobile strike forces to pursue ordinary criminals—or even pirates who have fled
the sea—onto the land territory of another state.

Down to the early twentieth century, commentators on international law
acknowledged that, where pirates could not be apprehended and subjected to
criminal justice, it was lawful for naval warships to resort to military action
against pirate ships, even if pirate ships would be sunk and many on board
would lose their lives. It was not necessary to show that pirate ships were an
immediate threat at the time of the attacks, in contrast to the rules regarding use
of force against suspected criminals on land.

In recent years, as the threat of piracy has revived, off the Horn of Africa
and elsewhere, the UN Security Council has revived the older approach,
expressly (and repeatedly) authorizing the world's navies to fire on pirate ships
that refuse to surrender. The Security Council has never authorized missile
attacks on land targets, even in its many resolutions calling for cooperation in
resisting terrorism. Part of the reason, surely, is that strikes at sea raise fewer
questions about collateral damage to innocent civilians.

52 The Convention authorizes warships to send boarding parties to inspect foreign flagged merchant
ships on the high seas only when there is

[Reasonable ground for suspecting that: (a) the ship is engaged in piracy; (b) the
ship is engaged in the slave trade; (c) the ship is engaged in unauthorized
broadcasting [and connected to the flag state of the warship] . . . ; (d) the ship is
without nationality; or (e) though flying a foreign flag . . . the ship is, in reality, of
the same nationality as the warship.

UN Convention on the Law of the Sea, Art 110 (cited in note 51). Articles 101-07 specify other
rights and responsibilities of warships in dealing with pirate ships. All other categories in Article
110 are only covered in isolated, one-off provisions.


54 See Nicholas Poulantzas, The Right of Hot Pursuit in International Law, 11-12 (Kluwer 2002) (because
"states are very sensitive to incidents involving . . . unauthorized crossing of their frontiers . . .
pursuit on land has not succeeded in acquiring the character of a right in customary international
law, as is the case with hot pursuit in the international law of the sea"). But even at sea, piracy is a
special case: see Douglas Guilfoyle, Shipping Interdiction and the Law of the Sea (Cambridge 2009), 28-
45 (even "factually piratical acts committed in territorial waters are not, at international law,
piracy"—so pursuit by third parties is not lawful, though it might be for immediate victims of a
pirate attack).


In sum, the world has, in many different ways, recognized different rules for the use of armed force on the seas than on land. We may think of cyberspace as an arena of armed conflict or of something akin to it. We should not, for that reason, assume that cyber attacks should be covered by the same rules that apply to conventional war on land. In many ways cyber conflict is more like naval warfare or deployment of force on the seas. That does not mean that no rules apply to cyber operations. Military operations at sea were never allowed to proceed without limiting rules. As with the use of force at sea, we should expect cyber operations to follow a law distinct from that of land warfare.

III. ARMING MERCHANT SHIPS AND OTHER INSTRUCTIVE ANALOGIES

Before turning to more detailed considerations of legal norms for cyber conflict, it is worthwhile to examine in some detail the legal disputes provoked by new naval tactics in the world wars. These episodes also offer instructive analogies with current disputes about permissible tactics in cyber conflict. In particular, they highlight the differing responses likely to flow from generalized attacks on civilian property, compared with immediate threats to the life or health of civilian persons.

At the outbreak of war in 1914, Britain and France sought to blockade German ports. Within months, they announced an expansion of the blockade to prevent shipping of contraband to nearby neutral ports (from which cargoes might be carried overland to Germany or its allies). The Allies then steadily expanded the list of items to be treated as contraband, ultimately including even supplies of food.\(^5\) Early in 1915, Germany announced a countering exclusion zone in the waters surrounding the British Isles.\(^6\) To enforce this policy, Germany asserted the right to launch submarine attacks on all shipping in the prohibited area. Eventually it expanded the prohibited area to the whole of the Atlantic.

The new term “economic warfare” came into use to describe these rival measures. They were much more encompassing than blockades in most earlier

---


wars, which had focused on closing specific ports or blocking imports of militarily related “contraband.”

If their strategic logic was comparable, the tactics adopted on each side did not operate the same way in practice. Allied blockade measures were enforced with surface war ships, which could divert merchant ships to Allied ports for closer inspection and sometimes seize both ship and cargo as prize of war. German U-boats could not seize control of foreign ships on the high seas.

In practice, submarines could not even safely approach a merchant ship if the latter were prepared to defend itself. The thin hulls of submarines made them very vulnerable to attack, even from small caliber guns, as well as to ramming by surface ships. So submarines usually struck without warning, often leaving too little time for crew and passengers on the target ship to escape to lifeboats. When they managed to sink a ship, submarines did not have the space to take on survivors. Submarine warfare therefore looked like sheer slaughter on the seas, extending not only to naval crews but also to civilians.

Attacks without warning provoked immense indignation, particularly when the victims were neutrals. The sinking of the British passenger liner Lusitania in 1915—a ship which included American citizens among its passengers—provoked such intense protest from the neutral United States that Germany agreed for a time to suspend such attacks. When Germany announced a

59 See Stevenson, Cataclysm at 201 (cited in note 57) (explaining the term “economic warfare” with a summary of the differences with past practice).

60 See Paul Halpern, A Naval History of the First World War 202 (Naval Institute 1994).

61 Id at 296.

62 Id.

63 Halpern writes:

[J]whereas British and French actions involved property and could be contested in prize courts, the German measures in the submarine war frequently involved loss of life. Neutral and other shipowners might on occasion win awards for damages or restoration of their property in prize courts, but a life, once lost, could never be restored. The British and French therefore had a noted advantage in the propaganda war for the sympathy of the richest and most powerful neutral of them all, the United States. The Germans—at least the naval authorities—however well grounded and legalistic their arguments, seemed never to fully comprehend this.

Id at 291–92.

64 See Charles Cheney Hyde, Attacks on Unarmed Enemy Merchant Vessels, 11 Am Socy Intl L Proc 26, 31, 36 (1917). At a conference sponsored by the American Society of International Law in the spring of 1917, one scholar denounced German practice as “wanton disregard of unoffending human life.” Another compared the U-boat campaign to the “atrocities” practiced at Andersonville Prison during the Civil War by its commander, Captain Wirtz—who, the audience was reminded, “was himself a German-Swiss.”

65 Richard Hough, The Great War at Sea, 175–77 (Oxford 1983) (describing initial German efforts to defend the sinking of the Lusitania, starting with the plea that Americans had been warned not to travel to Britain by notices placed in New York newspapers, after which German “government
resumption of such attacks in 1917, it provoked American entry into the war on the Allied side.\textsuperscript{66}

Allied indignation was still so strong after the war that Britain demanded a total ban on submarines.\textsuperscript{67} The United States proposed that commanders who ordered attacks on civilian shipping without warning should be treated as pirates.\textsuperscript{68} Though it did not go quite so far, the Washington Naval Treaty of 1922 restated the rule that all ships—including submarines—must give warning to merchant ships before attacking.\textsuperscript{69} The 1936 agreement on submarine warfare reemphasized the restriction and Germany was among the states that agreed to these terms.\textsuperscript{70}

Nonetheless, at the outset of the Second World War, Germany immediately resumed the practice of submarine attacks without warning.\textsuperscript{71} At the post-war Nuremberg trials, Admiral Karl Doenitz, commander of the U-boat fleet, was sentenced to twenty years in prison for ordering his U-boats to fire on shipwrecked crews, struggling in the water after their ships had been torpedoed.\textsuperscript{72}

Allied indignation against indiscriminate attacks by U-boats is all the more notable because the Allies were simultaneously imposing much strain on German civilians through ever tightening blockades. In both world wars, far more civilians may have died from the Allied blockades (when food shortages led to starvation and disease) than were killed or injured by U-boat attacks on

\textsuperscript{66} Stevenson, \textit{Cataclysm} at 261 (cited in note 54) ("Unrestricted submarine warfare was an essential cause of American entry [into the World War] and not simply a pretext for it.").


\textsuperscript{68} Id.

\textsuperscript{69} Id.

\textsuperscript{70} For debates in the inter-war period, see Levie, 65 Intl L Studies Ser US Naval War Coll at 28 (cited in note 67).

\textsuperscript{71} The British passenger liner \textit{SS Athena} was sunk by a German U-boat within nine hours of Britain's declaration of war in September 1939. The U-boat fleet had been deployed for such attacks even before the formal initiation of hostilities. Roberts, \textit{Storm of War} at 35 (cited in note 31).

\textsuperscript{72} See Taylor, \textit{The Anatomy of the Nuremberg Trials} at 399–409 (cited in note 32) (At British insistence, prosecutors pursued charges against Doenitz for directing U-boat attacks on civilian shipping without giving warning to the targets. After Doenitz's lawyers produced statements from American admirals acknowledging that the US Navy had embraced similar tactics against Japanese freighters in the Pacific, the Tribunal refused to impose separate punishment on Doenitz on this charge.).
the high seas. But the effects of the Allied blockades were indirect. They might have been alleviated by greater efforts on the German side to distribute declining food stocks more equitably. The U-boat attacks looked more terrible at the time, because there was so little that could be done to rescue passengers and crews on sinking ships in mid-ocean.

Again, the analogy with cyber conflict is very clear: cyber attacks can disable equipment and cause considerable economic damage, without causing direct threats to civilian life. It is certainly possible for cyber attacks to cause loss of life, even large-scale loss of life. But that consequence is not inevitable. Cyber attackers can choose to keep attacks below the level at which they trigger humanitarian catastrophe. Even in a full-scale conflict, attackers will often have definite incentives to exercise such restraint, to avoid provoking retaliation in kind. Even below that threshold, however, cyber attacks can exert a great deal of pressure on an opposing state, not least by diverting a government’s attention to coping with indirect harm to civilians. Such effects cannot be automatically condemned as in violation of humanitarian constraint, since official UN sanctions—such as limitations on trade with a target state—proceed by exactly the same mechanism.

73 Germany estimated some 700,000 civilian deaths were caused or hastened (as hungry civilians succumbed to disease) by the Allied blockade in the First World War. Alexander Gillespie, 2 A History of the Laws of War: The Customs and Laws of War With Regards to Civilians in Times of Conflict 73 (Hart 2011). But see Niall Ferguson, The Pity of War 277 (Basic Books 1999) (rejecting the 700,000 figure as “fantastic” and insisting that there is “no evidence that anyone starved” in Germany as a result of the blockade, though it is clear that there were severe food shortages which may have left civilians more vulnerable to disease in the last years of the war). Civilian deaths in 1918 were 29 percent above 1913 totals. Bruce Russell, Prize Courts and U-Boats, International Law at Sea and Economic Warfare during the First World War 133 (Republic of Letters 2009). In Britain’s merchant navy—which carried by far the largest amount of freight and suffered the heaviest losses—U-boat attacks in the First World War took the lives of “nearly 15,000 merchant sea men.” Imperial War Museums, The Merchant Navy, online at http://www.iwm.org.uk/history/the-merchant-navy# (visited May 2, 2013).

74 The distinction was still compelling to some scholars decades later. See Robert W. Tucker, The Law of War and Neutrality at Sea, 50 Intl L Studies Ser US Naval War Coll 45, 71–73 (1957).

75 Through the end of the 1990s, economic sanctions imposed by the UN Security Council were estimated to have caused “excessive morbidity”—that is, death from the effects of induced shortages of food, medicine and other essential supplies, especially among very young, very old and otherwise most vulnerable parts of the population—in the tens of thousands and perhaps higher. David Cortright and George Lopez, The Sanctions Decade: Assessing UN Strategies in the 1990s 46–47, 73–74 (Lynne Rienner 2000) (providing many examples, including Iraq and Serbia). Leland M. Goodrich, Edvard Hambro, and Anne Patricia Simmons, Charter Of The United Nations; Commentary and Documents 311–14 (Columbia 3d ed 1969) (surveying the deliberations at San Francisco regarding Article 41 and reporting no concern that excessive sanctions might be improper or implicitly constrained by the Charter).
The experience of war at sea also teaches another lesson—that efforts at self-defense are likely to be viewed with sympathy, even when there are otherwise plausible questions about their status or propriety in strict legal terms. For the debate about submarine tactics in the world wars was partly driven by a different innovation—the arming of merchant ships.

By the mid-nineteenth century, civilian shipping, no longer threatened by pirates, had abandoned any form of armament. On the eve of the First World War, Britain announced that it would again place guns (naval cannons) on some of its merchant ships. The British insisted that the guns were only for defensive purposes. As a practical matter, it was the arming of merchant ships that made it impossible for submarines to give warning. Submarines then faced even more need to adopt stealth attacks, as merchant ships were equipped with devices to hurl depth charges and instructed to use them when they became aware of lurking submarines, without waiting for the latter to announce their intentions. The British also equipped some of their own merchant ships with neutral flags, intensifying uncertainty among submarine commanders about which ships could safely be given advance warning.

The Germans protested that the arming of civilian ships was essentially a return to privateering, hence a violation of the 1856 Declaration of Paris. In 1916, German authorities captured the captain of an armed British merchant ship, who had earlier fought off a German naval attack. German authorities executed the captain for being an unlawful combatant—hence, in the German view, engaged in conduct equivalent to piracy. Before the war, a leading British legal commentator had acknowledged that international law would regard

---

77 Id (noting that the practice actually started almost a year before the outbreak of war, not to counter the submarine threat but to prepare against attacks from German merchant ships that might be converted to auxiliary naval cruisers in wartime).
78 In the first year of the First World War, when most merchant ships were still unarmed, U-boats sometimes did give warnings and allowed targeted ships time to place crew in lifeboats. Hawkins, Starvation Blockades at 99–100 (cited in note 58). The practice did not last.
79 The practice was defended by Churchill as “the well known ruse de guerre of hoisting false colours in order further to baffle and confuse the enemy.” Winston Churchill, II The World Crisis 1226 (Odhams 1939).
80 Hawkins, Starvation Blockades at 100–01 (cited in note 58) (“[T]his heavy handed action made a martyr out of [the executed British captain]. It was not logical that U-boats could kill civilians, but civilians could not kill U-boats.”); for a parallel account, see Halpern, A Naval History of the First World War at 296 (cited in note 60).
merchant crews as pirates if they engaged in armed conflict, even with enemy warships, while otherwise failing to abide by restrictions applicable to warships.\textsuperscript{81}

In the midst of the World War, however, Britain did not want to reclassify its merchant ships as warships, for it could not then protest the German practice of attacking merchant ships without warning. Nor could Britain accept that its merchant ships must abide by restrictions on warships entering neutral ports.\textsuperscript{82}

So Germany did have a serious legal argument against the British practice of arming merchant ships. Some neutral countries also protested the practice, precisely because they saw it as a threat to the security of neutral shipping.\textsuperscript{83} But the British persisted because armed merchant ships were much more likely to survive an encounter with a submarine. Before the advent of convoys in 1917, the best means of protecting merchant ships was to equip them with defensive armament of their own.\textsuperscript{84}

The practical arguments for the British policy were hard to resist. The United States adopted the practice itself in 1917—even before it entered the war.\textsuperscript{85} In the 1930s, isolationists insisted that arming American merchant ships—and receiving armed British merchant ships in American ports for extended

\textsuperscript{81} Oppenheim, \textit{2 International Law} at 226, § 181 (cited in note 26) (arguing that while the ship “would be considered and treated as a pirate” ship, the crew could be “treated as war criminals to the same extent as private individuals committing hostilities in land warfare”).

\textsuperscript{82} See Levie, 65 Intl L Studies Ser US Naval War Coll at 65 (cited in note 67) (Under the 1907 Hague Convention XIII (Rights and Duties of Neutral Powers in Naval War, CIS 299, Arts 12, 24) neutrals were prohibited from providing bases to warships of belligerent powers, thus required to limit visits from such warships to twenty-four hours. That limitation would be a severe problem for merchant ships, since it would not allow time enough to unload a full cargo and then reload.).

\textsuperscript{83} German objections are surveyed in A. Pearce Higgins, \textit{Armed Merchant Ships}, 8 Am J Intl L 705, 714–16 (1914); neutral concerns are described in Levie, 65 Intl L Studies Ser US Naval War Coll at 36 (cited in note 67).

\textsuperscript{84} Churchill, \textit{2 World Crisis} at 1229 (cited in note 79) (reporting that during 1916, “defensively armed” merchant ships escaped unharmed in 76 percent of their encounters with U-boats (673 out of 310), whereas only 22 percent of “unarmed ships” managed to escape such encounters (678 of 302), and the overwhelming majority of “unarmed ships” (235 of 302) were sunk in these encounters). An American historian concludes that in the last years of the war, the policy of arming American merchantmen also proved “surprisingly successful,” with 384 freighters and tankers using their guns to fight off U-boat attacks. Robert W. Love, \textit{History of the US Navy} 481 (Stackpole 1992).

\textsuperscript{85} President Wilson proposed the arming of US merchant ships in February 1917, then implemented the policy a few weeks later (after an overwhelming vote to approve this recourse in the House of Representatives)—a full month before the formal declaration of war. \textit{Declaration of War Against the Imperial German Government}, 11 Am J Intl L 349, 352 (1917).
stays—had compromised American neutrality and should not be repeated in the event of a future war. The argument fell on deaf ears.

At the outset of the Second World War, Britain again armed its merchant ships. They were received in American ports on the same terms as civilian shipping from neutral nations. As the U-boat menace intensified, the United States finally directed the arming of its own merchant ships and again did so before American entry into the war as a full belligerent. But even before that, neutral opinion, certainly in the United States, viewed the arming of merchant ships with indulgence. The practice seemed to draw moral warrant from the immediate claims of self-defense, a right which public opinion assumed even civilians were entitled to exercise when they could do so without immediate risk to other civilian lives. U-boats attacks continued to be viewed as wanton, because of their immediate and inescapable threat to civilian life.

86 "The [Wilson] administration had no intention of being neutral... and I fear it dragged our unwilling people into the war... On the armed merchant question, we took the position that armed belligerent merchantmen were peaceful vessels and could not be attacked." Statement of Professor Edwin Borchard in Proceedings of the American Society of International Law at Its Annual Meeting, 31 Am Socy Intl L 170, 173 (1937). Borchard held to the same view at the start of the next war. Edwin Borchard, Armed Merchantmen, 34 Am J Intl L 107 (1940).

87 Congress amended the 1936 Neutrality Act to allow arming of US merchant ships on Nov 17, 1941—three weeks before a formal declaration of war. The politics are described in Samuel Eliot Morison, 1 History of US Naval Operations in World War II: Battle of the Atlantic 296–97 (1975).

88 Thus, legislation enacted at the outset of the Second World War authorized the President to place restrictions on the use of the ports and territorial waters of the United States by submarines or armed merchantmen of a foreign state. 22 USC § 441. President Roosevelt implemented the measure by issuing a ban on submarines in American waters—but not on armed merchantmen. Some legal commentators raised objections, but the policy of treating armed merchantmen as “peaceable cargo ships” actually “occasioned little comment” in general public debates. Levie, 65 Intl L Studies Ser US Naval War Coll at 52 (cited in note 67). After U-boats attacked American naval escorts of merchant ships in September 1941, President Roosevelt denounced the U-boats as “rattlesnakes of the Atlantic,” insisting that defensive measures against U-boats (that is, direct attacks on the submarines) were permissible, even for a neutral (as the United States then was). A few weeks later, Roosevelt persuaded Congress to authorize arming of US merchant ships—when the United States was still far from committing to full-scale war (so far as was known at the time). David M. Kennedy, Freedom from Fear, The American People in Depression and War, 1929-1945 at 497–99 (Oxford 1999).

89 "A merchantman sailing the seas has a right to defend his property.... There is the further right of self-preservation..." Chandler P. Anderson, Ellery C. Stowell, and Maurice Leon, The Status of Armed Merchantmen, 11 Am Socy Intl L 11, 22 (1917). As the French jurist Jean-Etienne Portalis put it, "Armament for war is of a purely offensive nature.... But defence is a natural right, and means of defence are lawful in voyages at sea, as in all other dangerous occupations of life." Quoted in A. Pearce Higgins, Defensively-Armed Merchant Ships and Submarine Warfare 36 (Stevens and Sons 1917).
Here, too, there are obvious analogies with cyber conflict. Even at present, a vast range of civilian facilities are victims of cyber attack.¹⁰ In a more intense cyber conflict, there may be still more disruptive attacks, as much targeted on civilian infrastructure as on actual military facilities. We will want to emphasize the difference between attacks that merely impose harm and cost and those that threaten immediate loss of life—as might occur, for example, with attacks on hospitals or on a larger scale, from attacks on civilian aviation or on a still larger scale from attacks on controls for major dams. Some attacks ought to stir the special odium reserved for unrestricted U-boat warfare.

By the same token, however, civilian entities in our country may have special claim to defend themselves in the cyber realm. When it comes to defending against computer network attacks, even to engaging in some limited forms of retaliation, assigning some role to non-military participants should be considered as a permissible option. We did not, in the world wars, insist that merchant ships must simply remain exposed to attack, with no means to defend themselves, simply because they were not integrated into naval forces and not accorded the legal status of warships.

Another lesson of naval war in the twentieth century is that major powers have the decisive say about the rules. In the early years of both world wars, British and French decisionmakers worried a great deal about American reactions to their policies, especially on the high seas where American interests were most directly affected.¹¹ So in the first years of the First World War, they were cautious about tightening restrictions on neutral commerce with Germany.¹² Even German leaders gave attention to American reactions—though not enough. None of the powers gave much attention to protests from smaller neutral powers, such as the Netherlands and Sweden, whose shipping on the high seas was much constrained by Allied blockade measures.¹³

In both world wars, Allied powers ended up imposing a permit system on all neutral shipping, so that access to the Atlantic was dependent on a permit.

¹⁰ See Symantec, 18 Internet Security Threat Report 15 (2013), online at http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf (visited Apr 25, 2013). Cyber security firm Symantec found that in 2012 half of all major “targeted” attacks were aimed at either manufacturing firms (24 percent), finance, insurance, real estate firms (19 percent), or professional services (8 percent). Attacks on government agencies accounted for a mere 8 percent of these attacks.

¹¹ Nathan Miller, The U.S. Nag (Naval Institute 1997).

¹² For summary account, see Hawkins, Starvation Blockades at 83–89 (cited in note 58). For a more extended treatment, see Bell, Blockade of Germany at 265–75, 537–65 (cited in note 57). Among other things, the Allies negotiated agreements to allow neutral states in Europe to import American goods up to limits judged sufficient for their domestic use. See, for example, id at 309–16 (on shipping of American cotton).

¹³ See generally Bell, Blockade of Germany at 265–75, 537–65 (cited in note 57).
which could only be obtained by submitting to Allied inspectors in ports of embarkation, including even neutral ports. The system suited the needs—and could be enforced by the massed strength—of Allied powers at sea. Neutrals protested, but complied. The scale of Allied controls provoked criticism because it went far beyond anything attempted in previous wars. And it certainly restricted commercial opportunities. But Allied restrictions on neutral shipping did not provoke anything like the outrage stirred by U-boat attacks, because they did not threaten the lives of ship crews or passengers.

In like manner, there must be limits on cyber conflict in the twenty-first century to reassure bystanders that it will not quickly escalate to a level of intensity that threatens direct loss of life. But to insist on restraints is not to insist on the particular rules now generally assumed to apply to land warfare, which have come to demand a general exemption of “civilian objects” —that is, almost all elements of commercial traffic—from military measures. The lesson of war at sea in the twentieth century is that even neutral powers may accommodate defensive measures and strategic restrictions, if they are implemented in ways that do not imperil the lives of civilians. There are good reasons to respect humanitarian concerns, but “humanity” does not require policies exempting civilians from all costs of conflict.

IV. JUS AD BELLUM: WHEN CYBER RETALIATION IS JUSTIFIED

Much commentary on cyber attacks assumes that they may have strategic potential in warfare. The most alarmist commentary views cyber strikes not as the twenty-first century equivalent of German U-boats but as weapons comparable to nuclear tipped missiles or at least to a weapon of immediate strategic effect. Members of Congress and top officials have repeatedly warned about the threat of a “cyber Pearl Harbor.” The warning—and the seemingly irresistible analogy—was even embraced by the Director of Central Intelligence,

94 Hugh Ritchie, *The “Navicert” System During the World War* 3–4 (Carnegie 1938) (noting that part of the point was to ensure that supplies being shipped to neutral states such as the Netherlands were not going to be sent on to Germany by land).

Navigating Conflicts in Cyberspace

Leon Panetta, shortly before he became Secretary of Defense. Whether a cyber attack has that sort of strategic effect, it can certainly cause death and destruction on a large scale. A well-conceived attack might, for example, disable the US air traffic control system while hundreds of passenger jets were still in the air or disable the controls of a major dam system, flooding the surrounding area.

So the official “Cyber Strategy” of the United States, announced in May 2011, reserves the right to respond to a cyber attack with “military means.” That might well include retaliation with conventional—and highly destructive—bombs. Russian officials have proclaimed Moscow’s right to respond to a cyber attack with nuclear weapons. At the extreme, cyber war might look a lot like all-out war.

Viewed from this perspective, it might seem quite urgent to determine what sort of cyber attack would actually justify a full military response. A hostile power might, after all, simply penetrate US government computers to leave behind a taunting message, the equivalent of scrawling naughty words on the front fence. No one would think it reasonable to respond to such a prank with cruise missile strikes. There would be formidable legal objections to deploying

---

96 Leon Panetta invoked the analogy in testimony before the Senate Armed Service Committee, during hearings on his nomination to the post of Defense Secretary, having served more than two years by then as director of the CIA. Hearing to Consider the Nomination of Hon Leon E. Panetta to be Secretary of Defense, US Senate, Committee on Armed Services (June 9, 2011). For one account of the receptive reaction, see Anna Mulrine, *CLA Chief Leon Panetta: The Next Pearl Harbor Could Be a Cyberattack*, Christian Science Monitor (June 9, 2011), online at http://www.csmonitor.com/USA/Military/2011/0609/CLA-chief-Leon-Panetta-The-next-Pearl-Harbor-could-be-a-cyberattack (visited Mar 2, 2013) (Panetta arguing that the US would need to take defensive and offensive measures to prevent cyber attacks).


99 Hackers with a perverse sense of humor have played with the ambiguity of such “penetration.” On June 14, 2011, the US Senate’s website was hacked by a group calling themselves “LulzSec,” which posted this message: “This is a small, just-for-kicks release of some internal data from Senate.gov. Is this an act of war, gentlemen?” Andrew Morse and Ian Sherr, *Senate Website Gets Hacked*, Wall St J (June 14, 2011), online at http://online.wsj.com/article/SB10001424052702303848104576383970053018848.html (visited Mar 2, 2013).
conventional force in retaliation for an "attack" that was no more than the cyber equivalent of an adolescent prank.

The UN Charter obligates members to "settle their international disputes by peaceful means" and to "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state." The Charter gives broad powers of coercion to the Security Council and for the most part seems to give priority to the Council in deciding how armed force should be deployed. If the Council has not called for wider measures, member states are limited to the exercise of "the inherent right of individual or collective self-defense if an armed attack occurs."

Perhaps understandably, therefore, many commentators have tried to pin down when a cyber attack might qualify as an "armed attack," triggering the "inherent right of self-defense" under the Charter. If we were preparing to respond with a whole range of war measures, we would want to be sure we were actually faced with something equivalent to the Japanese attack on our battle fleet at Pearl Harbor and not a minor act of vandalism. When outside hackers interfered with Estonian government computers, disfiguring pictures of government leaders and disabling some minor services, NATO did not go on red alert. All NATO states were pledged to assist that Baltic ally from "attack." But the cyber mischief did not seem to be that sort of "attack." On the other

---

100 UN Charter, Art 2, ¶ 3.
101 Id at Art 2, ¶ 4.
102 Id at Arts 39–50.
103 Id at Art 51.
105 Newly Nasal, The Economist (May 26, 2007) (describing attack on Estonian government websites); John Schwartz, When Computers Attack, NY Times WK1 (June 24, 2007) (discussing preparations for cyber warfare); Gadi Evron, Battling Botnets and Online Mobs: Estonia’s Defense Efforts during the
hand, some commentators insist that even if a cyber attack is severe enough to trigger the right to self-defense under Article 51, defensive measures can only be lawfully pursued while the attack is underway—since responses would not otherwise be needed to repel the initial attack. All such reasoning skirts the most vexing (and likely most pertinent) legal challenges. Many analysts have followed former Air Force Judge Advocate General (JAG) Michael Schmitt in looking to the level of damage actually caused by a cyber attack to determine whether it can be viewed as equivalent to an "armed attack." As Schmitt himself has pointed out, however, if an incoming cyber attack is not damaging enough to merit designation as an "armed attack," then a response in kind would also fall outside the sorts of "attacks" the UN Charter seeks to control. By the same reasoning, responses at a lower level might not be covered by prohibitions in the Charter against resort to "force."

Under whatever rubric, at any rate, we still have to decide when and how to respond to injuries and provocations in cyberspace. The legal issues may seem technical, but they are not hypothetical. For one thing, hostile or potentially hostile powers—including China, Russia, Iran and others—are known to be investing in cyber attack capabilities. More than that, they are already demonstrating their capacities by infiltrating computer networks in the United States, with much attention to defense and intelligence agencies and military contractors as well as other sensitive targets. They also seem to be encouraging criminal networks to develop their capacities.


The possibility that 'cyber attacks' can...amount to 'armed attacks' which may trigger the right of self-defense does not mean, however, that the possibility of exercising this right can be easily established. ... So far, the main difficulty seems to lie in the fact that it is normally not possible to identify the attackers and thus to attribute the attack to a particular actor within the necessary timeframe. ... Even if the source of an attack could be located, additional conditions must be fulfilled before the right of self-defense can actually be exercised. In particular, the attack must not be over but still ongoing. This will often be difficult to determine and the burden of establishing that the attack is still ongoing lies on the State that purports to exercise its right of self-defense.


See Lyons, Threat Assessment of Cyber Warfare (cited in note 48).

National Counterintelligence Executive, Foreign Spies (cited in note 9); Ellen Nakashima, US Cyber-Spying Report Points to China, Russia, Wash Post A1 (Nov 4, 2011); Ellen Nakashima and William

Summer 2013 223
At some point, failure to respond may project weakness or indecision, encouraging bolder moves. That is why, during the Cold War, there were numerous low-level proxy wars between Communist and Western powers. Places not of inherent importance might gain significance as arenas in which major powers signaled strength—or weakness—in facing challenges to local allies or clients. From central Africa in the 1960s to Central America in the 1980s, the United States sponsored rebel or guerrilla forces to resist client states of the Soviet Union. The United States was not prepared to risk all-out war in such places, but it was not willing to ignore the dangers of acquiescing to even localized Soviet expansion.

The strategic imperatives are clear enough. We want potential adversaries to know that if they cross a certain threshold, they risk triggering the full range of war measures. But we do not want to signal that any provocations below that threshold will be disregarded by us and so prove costless to those who undertake them. The UN Charter itself recognizes these distinctions. For all that Article 51 seems to make “the inherent right of self-defense” contingent on an “armed attack,” the Charter as a whole does not reflect a dichotomous view of provocations. It does not establish a special category in which forceful responses are authorized and then prohibit forceful responses in all others.

The Charter authorizes the Security Council to impose enforcement “measures” on states found to be committing “aggression.” But it also authorizes the Council to act against a state engaged in a lesser provocation—the sort of action the Charter describes as a “breach of the peace” or a “threat to the peace.” Meanwhile, the Charter authorizes the Council to impose a range of

---

110 Wan, China’s Denials on Cyberattacks Undercut, Wash Post A12 (Aug 24, 2011) (on video indicating state support for hacking operations directed at the US).

111 See the revealing concerns of NATO experts recorded in Schmitt, The Tallinn Manual at 53-55 (cited in note 13): The Tallinn group acknowledges a right of self-defense under Article 51 of the UN Charter to “a cyber operation that rises to the level of an armed attack” (rule 13) but then equivocates on permissible responses to “a series of cyber incidents that individually fall below the threshold of an armed attack.” It holds that if “the smaller scale incidents are related and taken together have the requisite scale,” there “are grounds for treating the incidents as a composite armed attack.” But some members of the International Group of Experts (including participants from the United States, Canada and various European countries) took the view that “cyber attacks” could only be regarded as an “armed attack”—in the sense of Article 51 of the UN Charter—if combined with other attacks involving “weapons.”

112 For one assessment, see Henry Kissinger, Diplomacy 773-75 (Simon & Schuster 1994) (emphasizing opposition to Soviet expansion, rather than support for democracy as an aim in itself, in explaining US policy in Central America and elsewhere in the 1980s).

113 Simma, 2 Charter of the United Nations at 1403 (cited in note 106) (“The prevailing view considers Art 51 to exclude self-defense other than in response to an armed attack.”).

UN Charter at Art 39.
countering measures, culminating in deployment of the armed forces of the member states in full-scale combat operations.\textsuperscript{114}

Before that, however, the Council may impose sanctions, which the Charter describes as “measures not involving the use of armed force”—that is, measures imposed prior to full-scale military conflict. Such “measures . . . may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication.”\textsuperscript{115} It is no leap to suppose that, if they had known about cyber communication in 1945, the drafters of the Charter might have specified “interruption” of Internet “communication” in this list of sanctions “not involving the use of armed force.”

So the Charter still recognizes the problem that challenged states before 1945: How to respond to provocations that don’t rise to the level of full-scale armed invasion? The short answer is that states found ways of responding to provocations that did not commit them to waging full-scale war. Any longer answer would notice that delivering such responses was one of the historic purposes of naval power. Navies could disrupt an enemy’s “communication” without seizing and holding any part of the enemy’s own territory. The disruptions could impose dissuasive force, without provoking the enemy to respond with all-out war, as seizing territory would likely do.

As noted previously (Section II) the US Constitution includes an express provision for exercising this kind of response. Article I, Section 8 authorizes Congress to “declare War” but also—and separately—to “grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water.”\textsuperscript{116} The wording implies that Congress might well authorize limited raids against hostile powers—for reprisal or capture—without going so far as to “declare war.” That was certainly the practice.\textsuperscript{117}

The Department of the Navy was established as a separate service in 1798. That was almost a decade after Congress provided the new federal government

\textsuperscript{114} Id at Arts 42-49
\textsuperscript{115} Id at Art 41.
\textsuperscript{116} US Const, Art I, § 8. Captures on “land” were not necessarily accomplished by different agents than captures on “water”: during the War of Independence, John Paul Jones used his privateering license to make captures on land—by leading seamen against an isolated manor house—as well as capturing ships on “water.” See generally Dennis M. Conrad, John Paul Jones, in E. Gordon Bowen-Hassell, Dennis M. Conrad, and Mark L. Hates, eds, Sea Raiders of the American Revolution: The Continental Navy in European Waters 42-46, 48-51, 54-69 (Naval Historical Center 2003).
\textsuperscript{117} C. Kevin Marshall, Comment, Putting Privateers in Their Place: The Applicability of the Marque and Reprisal Clause to Undeclared Wars, 64 U Chi L Rev 953 (1997) (arguing the President might authorize the practice in response to attacks by foreign naval forces—even without congressional authorization, let alone declaration of war).
with a War Department. Congress envisioned the Navy Department as filling a separate role from simply supporting the army in full-scale war. In fact, the Navy Department was no sooner launched than it was thrust into the middle of America's first foreign conflict after the War of Independence—a conflict in which only the navy took part.

It was the "quasi-war" with France, lasting from 1798 to 1800, provoked by French attacks on American shipping. Revolutionary France wanted to stop American trade with Britain. The United States wanted to defend its trading rights as a neutral. The two dozen ships of the US Navy were deployed to protect American merchant ships against French privateers, while American privateers were simultaneously unloosed against French merchant shipping. There was conflict, loss of property and some loss of life at sea, but there was no full-scale war. And it ended well, when France agreed to refrain from future attacks on American shipping in a treaty signed in September 1800.

The practice was already well recognized by international law treatises, where it was sometimes described as "imperfect war." A full account had already appeared in Principles of Natural and Politic Law by the Swiss scholar, Jean-Jacques Burlamaqui. That treatise was well known to the American Founders. Burlamaqui described "imperfect war" as one "which does not entirely [sic] interrupt the peace, but only in certain particulars, the public tranquility being in other respects undisturbed." Burlamaqui's treatise offers, as a premier example, acts of "reprisal" for a foreign power's injuries to a nation's own citizens.

In 1800, a case reached the Supreme Court about the status of a merchant ship that had originally belonged to Americans, then been seized by the French navy and finally rescued by the armed action of another (private) American ship. Was the liberation of the ship from French hands taking it "from the

119 Id.
121 For example, James Wilson, one of the most influential delegates at the Philadelphia Convention and subsequently among the first justices of the US Supreme Court, cited Burlamaqui with some regularity. The most recent edition of the Collected Works Of James Wilson contains ten references to Burlamaqui in the index (compared with twelve references to Vattel, eighteen reference to John Locke, and three references to Jean-Jacques Rousseau). Kermit L. Hall and Mark David Hall, eds, II Collected Works Of James Wilson 1222, 1242, 1254, 1260 (Liberty Fund 2007).
122 Burlamaqui, Principles, § 30, 475 (cited in note 120).
123 Id at § 31, 475.
124 Bas v Tingy, 4 US 37 (1800).
enemy” (as a 1799 statute required for determining the compensation to the ship "capture")? Not only was there no declaration of war against France, there was no act of Congress clearly designating France as "the enemy." Still, all the Justices agreed that seizing the ship from French control and restoring it to its original American owners was lawful. Following Burlamaqui, Justice Paterson described the conflict as an "imperfect war, or a war as to certain objects and to a certain extent" under which "national armed vessels of the United States are expressly authorised" to attack certain objects, for certain purposes.

While privateering at sea was repudiated in the mid-nineteenth century, the concept of "imperfect war"—or something akin to it—certainly was not. Subsequent treatises into the twentieth century and down to the present day described essentially the same practice under such rubrics as "armed reprisals" or "pacific reprisals." A more systematic response was "pacific blockade," shutting a foreign port in peacetime as a way of applying economic pressure on the targeted state.

Well into the twentieth century, naval deployments were used to intimidate a target state without necessarily committing to land invasion—hence the expressive term "gunboat diplomacy." A study published at the end of the century listed well over 200 episodes, between 1919 and 1991, in which peacetime deployments of naval force had been used to deter foreign states (or foreign nationals) from hostile acts. The challenge has endured, despite

---
125 Id at 42.
126 Id at 45.
127 See, for example, Oppenheim, 2 International Law at 47, § 42 (cited in note 26) ("States will have recourse to reprisals for such international delinquencies as they think insufficiently important for a declaration of war but too important to be entirely overlooked."). Oppenheim notes that letters of marque and other authorizations for private citizens to organize reprisals fell out of practice after the eighteenth century but states continued to use public force in somewhat similar actions: "An act of reprisal may be performed against anything or everything that belongs... to the delinquent State or its citizens." Id at 41, § 37. The term "pacific reprisals" does not imply absence of force or violence but the absence of a surrounding context of war, in contrast to "belligerent reprisals" conducted in wartime. For endorsement of such peacetimes ventures in limited military strikes for purpose of retaliation, see Michael A. Newton, Reconsidering Reprisals, 20 Duke J Comp & Intl L 361 (2010).
128 Oppenheim, 2 International Law at §§ 48-53 (cited in note 26).
129 James Cable defines "gunboat diplomacy" as "the use or threat of limited naval force, otherwise than as an act of war, in order to secure advantage or avert loss, either in the furtherance of an international dispute or else against foreign nationals within the territory or the jurisdiction of their own state." James Cable, Gunboat Diplomacy 1919–1991: Political Applications of Limited Naval Force 14 (St Martin 3d ed 1994). The list of episodes purports to be illustrative rather than exhaustive. Id at 157–213. Of these episodes, eighty-nine (more than one third) involved the US Navy, though often in joint actions with other western navies; more than half (163) took place
changes in diplomatic priorities: there are situations where security demands a response but not a war. In recent years, a few commentators have invoked the traditional term, "imperfect war," to characterize aspects of the "war on terror"—something that is more than law enforcement but less than full-blown "war."\footnote{Many commentators, it is true, hold that the UN Charter has superseded all such practices. In this view, international law now leaves exclusive control over all resort to "force" with the Security Council—unless a state is acting purely in immediate self-defense "when an armed attack occurs."\footnote{Gregory E. Maggs, \textit{Assessing the Legality of Counterterrorism Measures Without Characterizing Them as Law Enforcement or Military Action} (Public Law and Legal Theory Working Paper, George Washington University Law School, Feb 26, 2006), online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=965433 (visited Mar 2, 2013) (arguing that counterterrorism measures should be treated as a form of governmental action that is neither law enforcement nor military action); Kathryn L. Einspanier, \textit{Burlamaqui, the Constitution, and the Imperfect War on Terror}, 96 \textit{Georgetown LJ} 985, 988 (2007) ("The difference in the legal operation between declarations of war and engagements in imperfect war is the level of autonomy granted to the President to wage the war as Commander-in-Chief.").} It might be that such restrictions don't apply, in any case, to countermeasures in cyberspace, since (according to a plausible view) they do not qualify as "force" unless they are extremely destructive. Before reaching any firm conclusions on where to draw lines, we might usefully consider whether the United States actually embraces the restrictive understanding of the Charter, even when it comes to deployment of naval warships.

The same clause of the Charter not only commits members to "refrain in their international relations from the . . . use of force" but also from "the threat . . . of force against the territorial integrity or political independence of another state . . . ."\footnote{A leading commentary on the UN Charter puts it this way: "Lawful self-defense is restricted to . . . repelling of an armed attack and must not acquire a retaliatory, deterrent, or punitive character." Simma, \textit{Charter of the United Nations} at 1425 (cited in note 106).} Resolutions of the UN General Assembly have sought to emphasize that the Charter prohibits the "threat of force" along with the "use of force."\footnote{UN Charter at Art 2, ¶ 4 (emphasis added).}
Yet for all that, the United States has regularly deployed force in ways that involve an element of “threat.” Even in recent decades, the Navy has most often been the vehicle for delivering such threats. Seaborne threats do not require seizing and holding actual territory of the target state, so they do not look quite so much like a direct attack on the target state’s “territorial integrity.”

Consider the Cuban Missile Crisis, in which the Kennedy Administration deployed the Navy to impose a “quarantine” on Cuba, preventing the shipment of Russian missiles to the island. Less than two years before, the same administration had declined to provide direct US air support for an invasion of Cuba by anti-Castro rebels. The quasi-blockade, though controversial among legal analysts, was regarded as less clearly contrary to international norms since it operated at a distance, with limited force and with no immediate harm to civilians.

During the Iran-Iraq war in the late 1980s, the United States took “active measures” to protect international oil shipping, deploying the US Navy to the Persian Gulf. When US Marine helicopters spotted an Iranian ship laying mines in international waters, they attacked and disabled the ship. American naval forces subsequently seized control of the Iranian ship, removed its crew and then sent the ship to the bottom. Two Iranian naval frigates were subsequently sunk by missiles launched from American ships. The US never declared war on Iran, however, nor did the Reagan administration even acknowledge to Congress that the Navy was entering a “war zone.” But the presence of the Navy in the first place was an implicit threat to use force. In many minor episodes, a naval fleet has been deployed to a troubled part of the world to register American concerns. The deployment of an aircraft carrier is not usually seen as token of sympathy.

---

135 Id at 230–32. For contemporaneous debate, see Quincy Wright, *The Cuban Quarantine*, 57 Am J Intl L 546 (1963) (questioning legality of the measure, since not responding to “armed attack”); Abram Chayes, *Cuban Missile Crisis, International Crisis and the Role of Law* (2d ed Oxford 1987) (emphasizing the Kennedy administration’s reluctance to plead self-defense, for fear of setting a dangerous precedent, but still offering legal arguments justifying the naval response in this case grounded in approval from the Organization of American States).

It is... misleading to make any dichotomy between “peacetime presence” and “wartime” combat capabilities, since a “presence” can have no significant effect in the absence of any possibility that the transition to war will be made... Latent susion is therefore... likely to be the most important class of benefits generated by sea power... The deployment of naval forces is [also] a continuous reminder to allies and clients of the capabilities that can be brought to their aid.
There is, arguably, a continuum between reminders, threats, demonstrations and actual attacks. It is not always easy to draw lines between one stage and the next in the course of a confrontation. A warship may “fire across the bow” in a way that demonstrates capacity to attack without inflicting injury. What is the difference between firing such a warning shot and threatening to do so? In many situations, the difference may be a matter of emphasis or degree rather than a categorical distinction. Something similar might be said of an incident in which actual shots are fired at another vessel without causing loss of life or any serious injury or damage. Arguably such an action should properly be considered a more severe form of warning rather than an actual attack.

At the other end of the spectrum, merely sending warships into a zone of conflict (or into international waters adjoining the territorial waters of a hostile or potentially hostile state) might, in some circumstances, be seen as a threatening action, even if no explicit threat were expressed in words. If American ships were attacked, they would then claim to be acting in self-defense when resorting to force. Did the aggression start with the initial attack or with the provocative presence?

So, for example, when President Reagan sent a naval task force to the Gulf of Sidra in 1981, he had every reason to think Libya’s dictator, Muammar Qaddafi, would regard the appearance of American ships there as a provocation. Qaddafi had claimed the Gulf of Sidra as Libyan territorial waters. Though the claim was not well founded in international law, Qaddafi insisted it would violate Libyan sovereignty for ships to enter those waters without express permission from the Libyan government.138

Accordingly, the Defense Department instructed the task force to operate under “Reagan Rules of Engagement”: if they judged themselves under threat, local commanders were authorized to respond with force.139 Soon enough, they so judged and so responded. In the ensuing encounter, American fighter jets shot down two Libyan aircraft. The American claim to be acting in self-defense was denounced by the Soviet Union and other hostile states. Even traditional US allies declined to express full support.140 The United States still insisted it had been acting within its rights by defending its ships in international waters.141

The least one can say is that successive American presidents have not regarded the UN Charter as excluding the use of naval demonstrations to

139 Id at 46–47.
140 Id at 61–62 (only Egypt’s Anwar Sadat and Israel’s Menachem Begin expressed full support for US action in the Gulf of Sidra).
141 Id at 58–60.
dissuade potential adversaries from acting against basic American interests or commitments. The United States has considered that “threat” means something different at sea than it might on land. We have been prepared to deploy naval warships even when not prepared to land marines or launch cruise missiles. Even if a threat at sea does result in injury or damage or loss of life, the scope of the harm is more readily contained and less likely to lead to a larger war.

Everything that is true of naval power in these respects might very well be claimed for cyber reprisals. It is possible to imagine a range of countermeasures in cyberspace, ranging from the cautionary to the severely disabling. Even a severely disabling “attack” in cyberspace might cause no loss of life and no physical destruction. It might be highly disruptive without imposing permanent damage. If we classify every form of cyber retaliation as the sort of “armed force” that can only be exercised in response to “armed attack,” we forfeit one of the main advantages of cyber measures—their vast flexibility and potential for highly calibrated levels of intervention.

It is possible, of course, that even finely calibrated measures may provoke angry responses, so that measures and countermeasures escalate to dangerous confrontations. But failure to respond can sometimes be as dangerous as overreaction; a firm response can often serve as a sobering deterrent rather than an inflaming provocation. The risk that cyber measures will escalate to more destructive attacks should cause concern. It is not an argument against considering more options. Our current announced policy is to threaten to deploy conventional bombing in retaliation for a sufficiently severe cyber attack but not to clarify what happens before cyber attackers reach the line that might trigger that response.

Being willing to consider cyber responses does not mean we must be open to any and all forms of retaliation. To the contrary, given the potential destructiveness of cyber attacks, we should devote much effort to clarifying necessary limits and threatening severe penalties for attackers who exceed them. But to think about such limits, it is necessary to think a bit more concretely about how and where cyber reprisals might operate. It does not make much sense to think of them as analogues to war on land.

V. PERMISSIBLE TARGETS AND THE PROBLEM OF ATtribution

According to the ICRC, international law already has an established rule that forbids attacks on civilian infrastructure, even in cyberspace.\textsuperscript{142} The argument is beguilingly simple. It starts by invoking the most comprehensive

\textsuperscript{142} International Committee of the Red Cross, \textit{Cyber Warfare} at *1 (cited in note 12).
convention on the law of armed conflict, AP I. That convention articulates this “basic rule”: participants in international conflicts must “at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.”

AP I defines “military objectives” as all those targets whose “total or partial destruction” would offer “in the circumstances ruling at the time... a definite military advantage.” All “objects” which are not “military objectives” under this definition are then classified as “civilian objects” and may not be “the object of attack or of reprisals.” Thus, even when an enemy violates these restrictions, the defenders may not retaliate in kind, because the prohibitions forbid targeting civilian objects by way of “reprisal.” The ICRC acknowledges that “cyber warfare adds a new level of complexity,” but insists that the rule set down in AP I “can and must be applied also to cyber warfare.”

One obvious problem with this conclusion, in relation to American policy, is that the United States is not a party to AP I. In the Red Cross view, that poses no difficulties for legal analysis because almost all the provisions in AP I summarize existing customary law and customary law is binding on all states. In 2005, the Red Cross published a multi-volume study purporting to demonstrate this conclusion. Many commentators on cyber conflict take for granted that attacks on “civilian objects” are now forbidden by international law, even in the cyber realm.

The United States government expressly rejected the ICRC study as any reliable guide to customary international law. The ICRC study relies almost entirely on statements of intention by governments, many of which are clearly

143 Additional Protocol I, 1125 UNTS 3 (cited in note 35).
144 Id at Art 48.
145 Id at Art 52, ¶ 2.
146 Id at Art 52, ¶ 1 (emphasis added).
149 See note 14.
150 John B. Bellinger III and William J. Haynes II, A US Government Response to the ICRC Study Customary International Humanitarian Law, 89 Intl Rev Red Cross 443 (2007) (giving a formal response by the US to the ICRC’s study on customary international humanitarian law). Bellinger was the legal adviser for the Department of State under Secretary of State Condoleezza Rice and Haynes was general counsel for the Department of Defense. Id.
rhetorical or misleading. To accept the ICRC view, one must ignore a great deal of practice, both in earlier times and today. A number of major military states have not ratified AP I. A number of others have ratified only with major reservations—including reservations against the prohibition on reprisal. In practice, conflicts in the last thirty years have not demonstrated general respect for these rules, even when it comes to the use of conventional weaponry.

Whatever one concludes about applying AP I to particular land conflicts, there remains a much more basic objection against extrapolating its restrictions to measures in the cyber realm. As Section II demonstrated, AP I rules have not, in fact, been accepted even by major western states as appropriate limitations for conflicts at sea. Customary practice and modern treaties alike have recognized the claims of “humanity” or “humanitarian obligation” on the seas. Unrestricted submarine warfare, directed at civilian shipping, was regarded with such horror that it provoked American entry into the First World War. But the claims of “humanity” at sea meant trying to limit loss of life, particularly in regard to non-combatants. Humanitarian obligation was never understood to require a generalized exemption of “civilian objects” from military targeting.

Cyber targeting is much more like naval combat in several key ways. The first is that, like naval war, cyber conflict can be quite effective without risking significant civilian casualties. At sea, it was possible to seize a cargo ship without any loss of life. It was even possible, when a seizure was contested, to promise that the ship and the cargo would be returned—or its value made good—if a prize court subsequently ruled that the seizure was unlawful. In a somewhat

---

151 The ICRC is so careless in distinguishing between practice and mere rhetoric that it includes affirmations clearly belied by actual practice—such as Prime Minister Chamberlain’s 1939 renunciation of bombing that might injure civilians or statements of Saddam Hussein condemning use of chemical weapons. Jean-Marie Henckaerts and Louise Doswald-Beck, eds, 2 Customary International Humanitarian Law 146, 169 (Cambridge 2005). It even invokes statements by opposition politicians, criticizing government policy—and then treats the opposition criticism as somehow as authoritative as the government policy it criticized. Id at 310 (citing Australian Shadow Defence Minister press release stating that Article 51(5)(b) would prevent Australian ships from providing “naval gunfire support” to an amphibious military operation in Kuwait). In the same vein, it attributes authoritative status to criticism of government policy by mere NGOs, not capable of directing the actual practice of actual states. Id at 236 (citing Human Rights Watch’s use of the Article 52(2) definition of a “military objective”), 311 (citing the ICRC’s opinion that including the word “overall” in the Article 8(2)(b) definition of “collateral damage” was redundant), 367 (citing Amnesty International’s claim that “serious mistakes in intelligence gathering seem to have led to unlawful deaths” in the 2000 NATO bombings in Yugoslavia). Yet the introduction claims that the volume “catalogs practice of international humanitarian law.” Id at xxii.

152 See note 18.

153 For the early nineteenth century view, see W.A. Phillips and A.H. Reed, 2 Neutrality, Its History, Economics and Law The Napoleonic Period 11 (Octagon 1976) (“The expediency of adhering to the law of nations, in the matter of the exercise of belligerent rights at sea, was recognized by all the
similar way, a cyber attack can be disabling without being irreversibly destructive. Many past cyber-attacks, for example, were “denial of service” attacks, where a website or computer system was rendered temporarily inaccessible but not otherwise damaged.\textsuperscript{154} Such attacks can result in economic loss or disruption, without imposing permanent damage or risks to human life.

One can argue that cyber strikes which do cause (or risk) loss of life should be seen as unlawful, by violating the principle of humanity. It does not follow that all cyber strikes against civilian objects must be seen as unlawful, any more than it follows that because unrestricted submarine warfare is condemned, all use of submarines must be banned or all civilian ships must be treated as exempt from military interventions. Claims for “humanitarian” restraint have always been understood as narrower than claims to a blanket principle of “distinction” for “civilian objects.”\textsuperscript{155}

Cyber weapons bear comparison with naval warfare at a still deeper level. The notion of a “military objective” set out in AP I—“definite military advantage” in “the circumstances ruling at the time”—implies something like a war in which control of particular sites is crucial for movement on land along a particular “front.” Control of a particular hilltop or bridge may offer “definite advantage” in “the circumstances ruling” at a particular stage of the fighting. The same site may lose that significance within a month, as contending armies maneuver to a different battlefront. In this setting, it makes sense to calibrate “definite advantage” in relation to “circumstances at the time.”

Naval war has usually been quite different. It has not aimed at controlling particular “fronts” but at imposing ongoing disruption to the enemy’s commerce or supply. Rarely could naval action be said to offer “definite military advantage” to combatants; for it was clearly not to their interest to turn neutrals into enemies by violating their acknowledged rights.”). Hence a famous British prize court ruling of the period held that the court’s duty was to determine neutral trading rights “exactly as if... sitting at Stockholm” (that is, capital of a leading neutral state). Id at 96. In fact, trade increased in almost all neutral ports during the period, id at 301, indicating the confidence of merchants in the restraints imposed by prize law.

\textsuperscript{154} See Cyber Security on the Offense (Ponemon Institute 2012), online at http://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/CyberSecurityontheOffense.pdf (visited May 13, 2013) (reporting that the average Denial of Service attack lasts only fifty-four minutes but that such attacks are still the highest concern of business owners); Symantec, 18 Internet Security Threat Report 17 (cited in note 90) (According to Symantec, such attacks are often launched as a “distraction” by criminals seeking to steal data, who find it convenient to divert the attention of IT staff while they “break into the company’s network.”).

\textsuperscript{155} See notes 18 and 28. As another example, see the restrictions on naval warfare adopted at the Second Hague Peace Conference, providing protections for captured crews, but not otherwise restricting the seizure of enemy merchant ships and their cargoes as prize of war. Convention (XI) Relative to Certain Restrictions with Regard to the Exercise of the Right of Capture in Naval War, 205 CTS 367–80 (1907).
in “circumstances ruling” at one stage of a war but not another. Blockades have
tended to be commitments for the duration of the conflict. Commanders could
rarely estimate what “advantage” was obtained from the blockade in any
particular month, since effectiveness was bound to be contingent on many
outside factors (relating to reliability of alternate supply routes or the availability
of domestic substitutions for imports). The effects of a blockade would be
cumulative, not to be judged by results in the “circumstances ruling” in any one
month.

Historically, the flexibility of naval forces allowed intervention at sea to
serve as a substitute for all-out war. It can be argued that even a blockade may
be more “humane” than full-scale invasion.\(^{156}\) It was certainly more flexible—in
the sense that it could be suspended at short notice and could allow for special
exemptions on transit across the blockade line, in ways that would be harder to
implement on a land front. Again, cyber weapons have the capacity to offer this
kind of more “humane” war.

In a more intense conflict, cyber weapons might actually trigger unsought
escalation if targeted at military controls. If we disable an adversary’s
communication, we make it hard for central commanders to tell outlying units
what to do. The response might be a welcome paralysis. Or it might, instead,
provogue a panicky response from lower level commanders as they sense
themselves slipping from the fog of war into total darkness. In a conflict where
the opposing side has weapons of mass destruction, would it be prudent to
undermine central control? During the Cold War, the United States went to
considerable trouble to exchange understandings and pointers with Soviet
counterparts on command and control strategies—to limit the risk that local
commanders might set off missiles in a panic of isolation.\(^{157}\)

What is true at the strategic level might be true at lower levels. In an all-out
war, it might be advantageous to disrupt communication systems on enemy
ships, even to disable their internal controls. But before that stage, we might find
it prudent to leave adversaries with reliable communication so they can respond

\(^{156}\) See, for example, *Commander’s Handbook on the Law of Naval Operations*, § 7.7.3 in Horace B.
Neutral vessels and aircraft in evident distress should be authorized entry into a
blockaded area and subsequently authorized to depart, under conditions prescribed
by the commander of the blockading force. Similarly, neutral vessels and aircraft
engaged in the carriage of relief supplies for the civilian population and the sick and
wounded should be authorized to pass through the blockade.

See also id at 137, (commentary by A.V. Lowe) (explaining that “[t]he *Commander’s Handbook* and
the Contemporary Law of the Sea” emphasize “humanitarian considerations” and justifying these
exemptions on such grounds, more than technical requirements of established law).

1990).
with suitable caution to an oncoming American fleet or understand that an aerial squadron is not bent on their immediate destruction.

In any lesser conflict, particularly a conflict which is primarily engaged at the cyber level, it would be a tremendous escalation, in fact, to start threatening the other side’s control of its own military assets. A conflict in which each side confines its attacks to the cyber realm may or may not be properly described as an “armed conflict.” Even if one grants the appropriateness of that designation, it is not at all easy to specify what would be a proper “military objective” in an “armed conflict” of that kind.

Suppose a cyber attack shuts down a significant part of the computer networks that process checks through the American banking system. Such an attack could impose very substantial cost and disruption without any immediate loss of life or limb. What would it mean to limit our response to relevant “military objectives”? Would we strike the particular computers from which the attack originated? What if (as is likely) that would make no difference to the capacity of the other side to launch parallel attacks from other computers? To ensure the enemy could not respond, would we try to disable all computers or computer networks in the country from which these attacks originated? Surely that would do vast harm to civilian infrastructure, perhaps to a degree quite disproportionate to any “definite military advantage.” We might think it not only more humane but more effective to fall back on the historic use of naval force—applying indirect economic pressure by targeting civilian infrastructure in a selective way in the target country.

What if, as is more than likely, we don’t know the precise origin of an attack? A good deal of literature worries about the “attribution problem” in cyber conflict.\textsuperscript{158} It is certainly true that actual perpetrators of computer network attacks can be hard to locate with precision or with perfect confidence. Network traffic can be routed through intermediaries. These intermediaries will often be unwilling or unable to help pin down the ultimate source of a malicious message. Destructive code can also be inserted into the target computer using a thumb drive. An enemy agent, infiltrated into the relevant facility, might be the culprit deploying that thumb drive. Or it might be introduced by a loyal but unwary

\textsuperscript{158} Barkham, 34 NYU J Intl L & Pol at 98–109 (cited in note 104); William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds, Technology, Policy, Law, and Ethics Regarding US Acquisition And Use Of Cyberattack Capabilities 1–18 (National Academies 2009); Graham H. Todd, Armed Attack in Cyberspace: Detering Asymmetric Warfare with an Asymmetric Definition, 64 AF L Rev 65, 93–98 (2009) (discussing the inadequacy of jus ad bellum in light of the increased difficulty in identifying sources of cyber attacks); Hollis, 52 Harv Intl LJ at 397–403 (cited in note 16) (arguing that current law cannot regulate cyber warfare because of the anonymous nature of the Internet); Erik M. Mudrinich, Cyber 3.0: The Department of Defense Strategy for Cyberspace and the Attribution Problem, 68 AF L Rev 167, 190–205 (2012) (discussing the strategy adopted by the US Department of Defense regarding operations in cyberspace and the attribution problem).
Navigating Conflicts in Cyberspace

local operator, transferring data between his office network and his personal laptop, after the latter had been penetrated by outside hackers. How can we hope to retaliate if we don’t know who has hit us?

But that is a very unlikely scenario for a “cyber Pearl Harbor.” The planes that actually struck the American fleet at Pearl Harbor had very clear Japanese markings. The Japanese government did not want the United States to be in doubt about the source of the attack because it wanted the United States to realize that it must change its policy toward Japan. Even terrorists usually claim responsibility for their attacks, because they want to indicate that such attacks can be avoided by abandoning a particular policy. Someone who simply wants to spread fear through random destruction can do so without resorting to computer technology—as proven, for example, by John Allen Muhammed and Lee Malvo, the sniper team that killed ten in the Washington metropolitan area in the fall of 2002, using an ordinary rifle.

We can, however, imagine a foreign state prepared to support or encourage cyber attacks without wanting to be held responsible for them—just as the Soviet Union encouraged terrorist groups in western Europe during the 1980s (including the Italian Red Brigades and the German Red Army Faction) and Islamist terror forces have received support from some governments in recent years. The cyber equivalent is no longer a mere hypothetical possibility. There are many reports that China and Russia have provided assistance to non-government groups engaged in cyber attacks on American companies. The

159 Gordon W. Prange, At Dawn We Slept 506 (McGraw Hill 1981). Shortly before 8:00 AM on December 7, 1941, Rear Admiral William Furlong, commanding Battle Forces Pacific at Pearl Harbor, heard the sound of an airplane engine, followed by the sound of a detonating bomb, and assumed it came from a “stupid, careless pilot” of an American aircraft until he “saw the red ball of the Rising Sun on the plane] and reacted instantly. ‘Japanese! Man your stations!’ he shouted.”

160 Japan could hardly have disguised its action, in any case, since the aerial attack on Pearl Harbor was followed up by landing Japanese troops to seize US bases in the Philippines. But Admiral Isoroku Yamamato, champion of the Pearl Harbor attack in Japanese strategy deliberations, insisted it was Japan’s “best claim for glory” so wanted his planes recognized. Roberts, Storm of War at 188 (cited in note 31).


lines readily blur between private crime and official surveillance, between extortion for private gain and harassment as calculated tactic of state policy.

Much discussion of the attribution problem focuses almost exclusively, however, on the difficulty of reliable attribution by technical means—computer forensics. Private companies may indeed be limited to such means. Governments are not. Governments have many methods of gathering intelligence, which can often provide strong indication that a particular state is involved with a particular set of cyber attacks. Defectors or leaked documents, for example, can provide strong evidence of culpability or at least intent. 164

At some point, it might be appropriate to consider retaliation as a means of deterring attacks. Today, governments threaten criminal prosecution to deter destructive cyber attacks. But prosecution requires that particular defendants somehow find their way into the custody of the prosecuting state. In the cyber realm, perpetrators may be oceans away from the victims of their attacks and protected by a sympathetic government where they do live. Even if suspects somehow are apprehended, successful prosecution requires proof beyond a reasonable doubt. A government which has acquired incriminating information through secret informants or surreptitious surveillance may be most reluctant to reveal its sources and methods in open court, but have no means of building a convincing prosecution otherwise.

The obvious alternative is to focus not on the actual perpetrators but the enabling state. To implement that strategy, it would not be necessary to establish—let alone prove in public court—every link in the chain of command or support. A pattern of cyber abuse might be sufficient to justify some response. Long before we resort to actual military force, it would be sensible to try retaliation at the cyber level.

We might do so with the aim of pressuring governments, much as, in the past, we would deploy a naval fleet, threatening to disrupt commercial traffic at sea. If we insist that cyber retaliation must be targeted on “military objectives” whose destruction would offer “a definite advantage” in the “circumstances ruling at the time,” we would often have to forego any cyber response at all.

164 Owens, Dam, and Lin, Technology, Policy, Law, and Ethics at 41 (cited in note 158):

[T]oday’s information technology makes it easy for evildoers to act anonymously. . . . On the other hand, an actionable degree of attribution might be possible by making use of non-technical information. Policy makers seeking absolute or unambiguous technical proof that a specific party is responsible for a cyberattack will almost certainly be disappointed in any real-life incident, and may ultimately be forced to rely on non-technical information more than they would prefer. The bottom line is that it is too strong a statement to say that plausible attribution of an adversary’s cyberattack is impossible, but it is also too strong to say that definitive and certain attribution of an adversary’s cyberattack will always be possible.
Neither security nor humanity would be served by diverting the response to cruise missile attacks on military formations.

Would we actually be retaliating in kind if our government responded to provocations delivered by civilian volunteers or criminals with counterattacks from US military computers? In this area, too, we will have to think more creatively if we want to avoid restricting our choices to equally unpalatable options.

VI. WHO ARE LAWFUL COMBATANTS IN CYBERSPACE?

If we think of cyber conflict as something like war, it may seem to follow that only uniformed combatants, under regular military command, can participate. A number of commentators insist that the law of armed conflict requires limiting participation in combat operations to actual uniformed military personnel. 165

At first glance, history might seem to be on their side. Even in war at sea, privateering has been considered unlawful since the mid-nineteenth century. During the American Civil War, the Confederate States did authorize ships to raid Union commerce on the high seas—but the Confederate government took the precaution of inducting these sea raiders into the official Confederate Navy, so they could not be charged with privateering. 166 Even so, the United States government held that, if captured, Confederate raiders should be treated as pirates, not as prisoners of war. 167

But restrictions on privateering took place in a world where almost all states had endorsed an international agreement repudiating the practice or demonstrated by their own actions (as the United States government did) that they would not authorize private attacks on enemy commerce. 168 The opposite is true in cyberspace.

Even in land warfare, the trend in the twentieth century was to be more accepting of auxiliary units, militia, and volunteers if they engaged in organized

---


166 Miller, The U.S. Navy at 133 (cited in note 91).


military operations though not part of the regular military.\textsuperscript{169} AP I actually grants prisoner of war protection to guerrilla fighters, even if they have no accountability to a government and conceal their status as fighters until the moment of their attack.\textsuperscript{170}

International law cannot reasonably be interpreted to take a more permissive stance toward guerrilla fighters, whose tactics often cause lethal injury to innocent civilians, than to cyber "attackers" who only damage property and equipment. And the main legal dispute regarding guerrillas—whether they are entitled to prisoner of war protection when captured—will not, in practice, arise with cyber attackers. Hackers do not need to have a physical presence within reach of those they target. They are, in fact, likely to be an ocean away.

As it is, the US government allocates some cyber operations to the NSA—as the efforts to undermine the Iranian nuclear program indicate. The restriction in the 2012 Defense Authorization Act, requiring offensive operations in cyberspace to conform to the "laws of armed conflict," applies by its terms only to operations conducted by the Department of Defense.\textsuperscript{171} There are no counterparts to that restriction in appropriations (or other legislation) affecting the NSA or other government agencies. Some targeting of drone strikes against

\textsuperscript{169} "The laws, rights and duties of war extend not only to armies, but also to militia and volunteer corps" when the latter are "commanded by a person responsible for his subordinates; . . . have a fixed distinctive emblem recognizable at a distance; . . . carry arms openly; and . . . conduct their operations in accordance with the laws and customs of war." Hague IV, 36 Stat 2277 at Annex I, Art I (cited in note 18).

\textsuperscript{170} Additional Protocol I, 1125 UNTS 3, at Art 44, ¶ 3 (cited in note 35):

Recognizing . . . that there are situations in armed conflicts where, owing to the nature of hostilities an armed combatant cannot so distinguish himself, he shall retain his status as a combatant entitled to prisoner of war protections, if captured provided that, in such situations, he carries his arms openly during each military engagement and . . . [when] visible to the adversary while he is engaged in a military deployment preceding the launching of an attack.

So combatants need not carry arms openly at other times. Not even this limited obligation has to be honored to secure protection: See id at ¶ 4:

A combatant who falls into the power of an adverse Party while failing to meet the requirements set forth in . . . Par 3 shall . . . nevertheless be given protections equivalent in all respects to those accorded to prisoners of war by [the 1949 Geneva] Convention and this protocol.

terrorists has already been entrusted to operatives of US intelligence agencies, rather than uniformed personnel in the military services.\textsuperscript{172}

The Obama Administration announced, in the spring of 2013, that it would transfer primary responsibility for drone strikes in battle zones from the Central Intelligence Agency to the Department of Defense. It did not concede that CIA participation in drone strikes would be unlawful or even that it would be entirely abandoned.\textsuperscript{173} Surely such drone strikes are closer to ordinary military action than cyber attacks. It would be odd to worry over civilian participation in cyber retaliation, while accepting civilian participation in actual missile strikes.

Even entrusting some retaliatory measures to private entities would not be unprecedented. The most obvious historical analogy is with the arming of merchant ships during the world wars. As described in Section III, there were serious reasons to question the legality of arming merchant ships while they still claimed some of the immunities of civilian shipping. Yet the practice came to be generally accepted because the claims of self-protection had so much moral force. At the same time, the threats this practice posed to third parties remained limited.

Much the same could be said of private enterprises which engage in hack-back activities against malicious hackers. Some American companies are already engaged in tracking of malicious hackers, identifying them to authorities, sometimes sending their own warnings and even minor forms of retaliation against hackers.\textsuperscript{174} Some commentators have urged that the practice be encouraged and expanded.\textsuperscript{175}

At a high level of abstraction, one might object that retaliatory actions by private companies make them participants in cyber conflict (or at least, in cyber strife or cyber abuse) and thus undermine their claims (as civilians) to remain immune from outside attack. But the same point applies to private companies in today's cyber realm as applied to merchant ships in the era of U-boats: they have


\textsuperscript{173} Mark Mazzetti and Scott Shane, \textit{As New Drone Policy is Weighed, Few Practical Effects are Seen}, NY Times A11 (Mar 21, 2013).

\textsuperscript{174} Brad Reed, \textit{Hacked Companies Start Hacking Back}, BGR (June 18, 2012), online at http://bgr.com/2012/06/18/anti-hacker-retaliation-new-policies/ (visited Apr 13, 2013).

already become targets. General Keith Alexander, current director of the NSA and commander of US Cyber Command, has endorsed estimates of the losses due to cyber theft of intellectual property as now reaching $250 billion annually—a loss he characterized as "the greatest transfer of wealth in world [history]."\textsuperscript{176} Others have estimated other losses to American business from cybercrime (other than from direct theft of intellectual property) at well over $300 billion per year.\textsuperscript{177}

Criminal gangs, often operating under foreign protection, now try to extort protection payments from vulnerable private companies—threatening to disrupt their services unless they make protection payments to the hackers.\textsuperscript{178} Then there is a vast amount of more direct theft, using so-called spider programs to transfer information—including patent or trade secrets—from owners to commercial rivals, most often in foreign countries (where their operations are not readily subject to legal recourse through US courts).\textsuperscript{179}

The most lucrative sorts of cyber-crime require a good deal of organization: specialists on breaking into insecure computer systems work with specialists on exploiting such break-ins, then these teams work with specialists on laundering money and so on.\textsuperscript{180} There are now private online forums serving a cyber black market, where specialists offer such services to would-be criminals.\textsuperscript{181} A criminal can purchase access to large numbers of hacked machines around the world—with prices varying from $8 to $180 per thousand


\textsuperscript{179} Office of the National Counterintelligence Executive, \textit{Foreign Spies} (cited in note 9).


hacked machines. What may interest criminal gangs may also interest governments, both for covert intelligence-gathering and harassing (or disabling) the security systems of rival states.

Characterizing such activities as crimes does not, in itself, do much to deter them. Attacks are not stopped by moralistic denunciations. They might, however, be significantly reduced by imposing costs on the attackers (or their state sponsors). That requires that victims—or potential victims—have some capacity to hit back at those who attack them. That was the historic remedy for depredations of commerce that transcended national borders.

Letters of reprisal—linked in the Constitution with letters of marque—arose centuries ago as a response to depredations that governments lacked the resources to prevent or even to punish. Merchants were issued letters of reprisal authorizing them to reclaim stolen property—or to compensate themselves by seizing assets of fellow countrymen of the original robbers. It was crude justice but it helped to establish limits on looting by predators operating under foreign protection. As the threat has returned, we should reconsider the historic means of responding and think about possible modern analogues. Modern navies have reduced the threat of piracy on the seas (except in a few especially troubled areas adjacent to failed states like Somalia). Modern security services have done little to protect private industry from cyber looting of intellectual property. Those with the most incentive to resist such depredations might have much to offer in helping to combat it—at the cyber level.

None of this, however, means that government could or should give up control of cyber strategy to non-government vigilantes. Private vengeance seekers—or thrill seekers—might provoke confrontations or inflame disputes, even where government officials judge that a more subdued response would be preferable. Private hackers might undermine standards of restraint which the government might otherwise hope to maintain, the better to invoke against foreign attackers.

But even in the world wars, there were clear lines distinguishing the role of naval warships from armed merchant ships. The latter were authorized to use force in self-defense while steaming from their embarkation ports to their assigned destinations. They were not authorized to perform naval missions on

184 For a general endorsement of the prevalent view from before the First World War, see Charles Cheney Hyde, 2 International Law: Chiefly as Interpreted and Applied by the United States § 709, 404–05 (Little, Brown 1922):
the side. They were armed to deal with the particular menace of U-boat attacks, not to deploy force for any of the objects that might be assigned to actual warships.\textsuperscript{185}

As the next section will discuss, there may be ways of emphasizing legal limits on the right of private retaliation in self-defense. But private firms are already under attack from cyber predators. Denying any right of self-defense is not a compelling strategy—any more than it would have been to leave merchant ships at the peril of U-boats. The fact that a cyber attack does not lead to loss of life might seem to make self-defense less urgent—but it also makes basic measures of self-defense less objectionable.

When it comes to crimes of violence, the law recognizes a right of self-defense. The Supreme Court has acknowledged that the right of self-defense encompasses a constitutionally guaranteed right to “bear arms” for personal defense.\textsuperscript{186} Private companies are allowed to hire armed security guards (and there are more security officers in private pay today than on public payrolls).\textsuperscript{187} It defies our general practice to insist that there remains no right of self-defense for victims of cyber attack. Leaving American private firms to swallow the costs without any chance at active defense is deserting them—and disregarding an important resource for bolstering our defenses. For the line between criminal

---

The exercise by a belligerent of the right to arm defensively its merchant vessels is doubtless associated with evils which maritime states have heretofore sought to remove from naval warfare. One of these is the commission of offensive operations by private ships oftentimes under private control.... The armed merchantman... becomes necessarily a participant in the conflict... but fails to satisfy the conditions imposed upon a ship converted into a naval auxiliary.

Nonetheless, Hyde acknowledged that when private vessels were “subjected to attack at sight by the submarines of a ruthless enemy,” the arming of merchant ships as “defensive measures” was “not to be questioned.” The second edition of Hyde’s treatise similarly acknowledged that German “methods pursued since the beginning of World War II... [featuring] the use of submarines [with] little deference for the law [regarding the rights of merchant shipping]... may again be deemed to necessitate the arming of American merchantmen.” Charles Cheney Hyde, 3 International Law Chiefly as Interpreted and Applied by the United States 1929, § 709 (Little, Brown 1945).

\textsuperscript{185} Levi, 65 Intl L Studies Ser US Naval War Col at 41 (cited in note 67) (“If it might be said that ‘defensively armed merchant vessels’ were properly so-called in that, unlike auxiliary merchant cruisers, they did not go searching for enemy vessels.”). Levi goes on to note that the designation “defensive” might be challenged since “they usually opened fire immediately upon sighting a U-boat.” Id.

\textsuperscript{186} District of Columbia v Heller, 554 US 570 (2008); McDonald v Chicago, 561 S Ct 3025 (2010).

\textsuperscript{187} It was estimated, within the past decade, that some two million security officers and guards were in private service, compared with 700,000 public police officers. Amy Goldstein, The Private Arm of the Law; Some Question the Granting of Police Power to Security Firms, Wash Post A4 (Jan 2, 2007).
gangs and government-sponsored predators is often quite smudged in the cyber realm, just as it often was when pirate ships stalked the open seas.\textsuperscript{188}

Most network infrastructure is privately owned. Companies like Verizon and AT&T, not the government, operate the Internet backbone.\textsuperscript{189} Unlike past land conflict, the domain of the conflict in a cyber war necessarily involves civilians. As a consequence, any computer security strategy will ultimately have to be implemented by these private parties. Giving them the discretion to innovate and to adapt the national strategy to their particular needs will help generate willing, as opposed to reluctant, cooperation.

And willing cooperation can be immensely valuable. Private companies and research institutions have far broader and deeper technical capabilities than the government alone can muster. US Cyber Command and the NSA have assembled teams of technical experts in computer science and network security, but private firms have more resources available. The annual revenue of one private security firm, Symantec, was $6.7 billion in 2011—about the same as the entire budget for NSA in 2006.\textsuperscript{190} The annual revenue of Microsoft was more than ten times that.\textsuperscript{191}

Private firms can offer much larger salaries to researchers and more desirable working conditions. Among other things, private researchers usually have more opportunity to exchange research findings with colleagues elsewhere—opportunities often restricted by security regulations applying to employees in government agencies. There is bound to be more technical talent outside the government than within its own cyber defense agencies. To limit the potential for private involvement in cyber security strategy is to forego a vast amount of potential reinforcement.

Organizations operating independently of governments—or directly against governments—in foreign countries may also have a valuable role to play in counteracting cyber abuses. Historic experience with land-based guerrilla forces offers some instructive analogies. During the Cold War, the United States encouraged anti-Communist insurgencies in many parts of the world. Support for the Contra rebels in Nicaragua in the 1980s even provoked a law suit before the International Court of Justice. In the ensuing decision, the ICJ scolded the

\textsuperscript{188} See notes 24 and 50.


United States for several aspects of its policy in Central America, but acknowledged that background support to rebels was not itself unlawful.\textsuperscript{192}

Just as foreign governments have sponsored or encouraged groups engaged in cyber harassment of American agencies and companies, there are foreign groups that might be very eager to engage in cyber operations against foreign powers. The most hostile foreign governments rule by authoritarian means and try to suppress all expression of dissent in their own territories. Accordingly, these governments try to prevent their own people from having access to free communication.\textsuperscript{193} They try to control Internet access. Dissident groups seek to break through government repression to spread their banned appeals. They are often eager to find means of circumventing network controls in these countries.

We might think of these groups as “irregular combatants in cyber conflict”—or “Internet Freedom Fighters.” The United States is known to have made modest efforts to assist such groups to evade Iranian government controls on Internet use.\textsuperscript{194} It might offer more help and provide it more widely. The \textit{New York Times} caused a stir in China when it revealed that relatives of the current premier had accumulated vast wealth.\textsuperscript{195} That information was not available to ordinary Chinese. Opponents of repressive regimes can apply pressure simply by publicizing forbidden information—and finding ways to preserve access to websites featuring such revelations, including personal secrets of the rulers.

Opposition websites may be illegal in authoritarian countries, but foreign repression measures are not binding law for the United States. Challenging such laws—not merely in public denunciations but in active counter-measures or encouragement to those engaged in active resistance in cyberspace—may be a

\textsuperscript{192} \textit{Nicaragua v. United States}, 1986 ICJ 139, 148 (June 27, 1986).

\textsuperscript{193} See Sanja Kelly, Sarah Cook, and Mai Truong, eds, \textit{Freedom on the Net 2012} (Freedom House 2012), online at http://freedomhouse.org/sites/default/files/resources/FOIN%202012%20-%20Full\%20Report_0.pdf (visited Apr 13, 2013) (showing that Internet regulation has increased in most countries and become increasingly sophisticated and more difficult to detect).

\textsuperscript{194} For an account of such assistance to Iranian dissidents, see John Markoff, \textit{With New Software, Iranians and Others Outwit Net Censors}, NY Times A1 (Apr 30, 2009). Technological assistance can not only help those who want to share information but those who want to receive it. The Naval Research Laboratory helped to develop “Tor,” a popular system that enables users to engage in web browsing without being detected by government surveillance. \textit{Tor Project, Overview}, online at https://www.torproject.org/about/overview.html.en (visited Mar 4, 2013).

very useful way of putting pressure on such governments. The people most active in such measures will usually be civilians. That should not pose any objection to supporting them.

But we can be more active in supporting such groups or less so. We can be vigilant to ensure they do not engage in vandalism or provocation—or we can be more indifferent to abuses that might be associated with such groups. As the International Court of Justice held in *Nicaragua v United States*, there is no direct legal liability for a state that aids groups that it does not directly control. The degree of our support for “cyber rebels” might be made contingent on cooperation from foreign governments in suppressing cyber criminals preying on American firms. That would be consistent with past practice in regard to actual guerilla movements.

Cyber insurgents are only one category of response that may raise thorny questions about legal status and accountability. The whole subject of liability and legal controls needs to be considered with care. It is a necessary foundation for any effective, sustainable cyber strategy.

**VII. LEGAL LIABILITY, POLITICAL RESPONSIBILITY**

As noted at the outset, the cyber realm is much like the high seas because, to begin with, both carry vast, economically valuable traffic. Powerful states and wealthy enterprises all around the world have much invested in maintaining the unobstructed flow of that traffic. That means that when conflicts spill into these “arenas,” there are (or will be) intense pressures to keep the conflicts from affecting third parties.

There are a number of ways in which cyber conflicts can produce spillover effects on third parties. The Internet relies on several pieces of distributed and shared infrastructure for its proper functioning. Domain names, such as www.uchicago.edu, are translated into the underlying IP addresses (like 198.101.129.15) by a system called the Domain Name System. The delivery of data to its intended destinations is managed by a system called the Border Gateway Protocol. Both of these systems rely on thousands of interlinked


197 1986 ICJ 139 (June 27, 1986).

198 Id at 148.


communicating computers, owned by private parties. Websites are authenticated by cryptographic certificates; hundreds of companies worldwide are involved in issuing and verifying these certificates. If any of these systems are disrupted, users would find websites inaccessible.

It will thus be extremely important—and strategically valuable—to isolate, stigmatize or at least clearly identify the powers that carelessly inflict harm on outsiders and those that do not. There will, of course, be attribution problems, confusion and ambiguity amidst misleading public denials and inconclusive intelligence reports. But such identification need not be perfect to be useful.

Efforts are already underway to mobilize international cooperation against cyber crime, notably through the European Convention on Cybercrime, known as the Budapest Convention. But many prominent states have declined to sign on to this treaty and not all signatories give full cooperation. Many states sponsor or encourage—or at least indulge—varieties of criminal activity in cyberspace, honing the capacity to engage in worse mischief for more strategic ends. We are not likely to see voluntary cooperation on a scale sufficient to suppress cyber crime because too many countries want to continue refining their capacity to deliver attacks in cyberspace.

One way to strengthen the confidence of third parties is to increase incentives for sharing information. That is one aim of the Budapest Convention. In effect, it now draws a line between states that have pledged to cooperate in tracking cyber threats—and expressed their commitment to do so by ratifying the convention—from states that have not accepted such obligations.

We do not now highlight this division in the world, however. Nor do we seem to provide strong incentives for states to align themselves with governments now seeking to control lawless interference with the Internet. Quite a number of malicious cyber intrusions have been traced to entities in China. The Chinese government routinely denies any involvement in such

201 Markus Jakobsson, ed, The Death of the Internet 156 (Wiley 2012).
204 Thirty-nine states had ratified the convention as of April 30, 2013, while another nine had signed but not yet ratified. See Council of Europe, Convention on Cybercrime, CETS No 185, Ratifications, online at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG (visited May 2, 2013). Non-signatory states include Russia, China, Iran, North Korea, Indonesia, India, and Pakistan—plus all states in Africa (apart from South Africa, which has signed but not ratified), all states in Latin America (other than the Dominican Republic), and all states in Asia (other than Japan).
attacks—but has never acknowledged responsibility to assist in identifying and punishing those who were involved.\textsuperscript{205} American protests have rarely been public and even more rarely given with particulars. The United States government might do much more to encourage cooperation with criminal investigations of Internet interference, both by promising sharing of information with participant states and exclusion toward others.

We cannot expect that all or most nations of the world will be prepared to participate in US countermeasures in cyberspace. Others may shrink from the costs or risks—and, as in other security fields, prefer to leave confrontation to American efforts. Still, the lessons of history are instructive. A central lesson of conflict on the high seas is that neutrals were much more accepting of war on the seas when their own interests were protected or at least generally accommodated. Thus, the practice of taking enemy shipping as prize of war was, for centuries, accompanied by the practice of letting neutrals challenge such seizures in special prize courts.\textsuperscript{206} War on the seas was allowed to proceed more aggressively than land war (at least in some respects) because it was still bound by legal limits.\textsuperscript{207}

If we think seriously about organizing the capacity to retaliate in cyberspace, we must think seriously about ways to develop and enforce legal limits, even on our own countermeasures. Such legal limits can operate in different forums and in different ways. They do not have to be perfectly calibrated or perfectly enforced to have some reassuring effect on third parties.

A first and most obvious response is to provide mechanisms by which government can immunize private entities cooperating with government agencies in countering cyber attacks. In the spring of 2012, Microsoft Corporation sought and received authorization from a federal court to seize domains and servers in Pennsylvania and Illinois, used to steal online banking information and move money from American accounts to controllers in foreign

\textsuperscript{205} Todd, 64 AF L Rev at 87–88 (cited in note 158).

\textsuperscript{206} James Wilford Garner, \textit{Prize Law During the World War} (Macmillan 1927), reports some 600 prize cases—overwhelmingly cases contesting seizures by Britain's Royal Navy—generally but not always upholding the legality of the seizure. In the \textit{Constantinos} case, the court ordered release of a Greek ship and its cargo, on the grounds that the Navy had wrongly applied retaliatory measures aimed at Germany to ships engaging in trade with Turkey. For collection of American cases, see James Brown Scott, ed, \textit{Prize Cases Decided in the US Supreme Court, 1789–1918} (Oxford 1923), reporting over 200 cases in some 2100 pages—but only one from the First World War and only forty from Civil War blockade enforcement.

\textsuperscript{207} “Prize practice was... widely accepted and supported by the international merchants of the world because it brought a valuable element of certainty to their dealings. The [remaining risks] could be covered by insurance.” Petrie, \textit{The Prize Game} at 145 (cited in note 19).
That approach, however, may prove too slow and cumbersome to be widely emulated. Even tracking the origins of attacks—the necessary basis for seeking a federal court authorization—might raise legal questions. Federal judges may not be in the best position to determine when and where such authorizations are appropriate, especially in the midst of fast-changing threat environments.

A better approach, therefore, might be to authorize a specialized executive agency, such as the NSA or a special unit in the Justice Department, to issue authorizations for private entities willing to undertake investigation of hackers and some sorts of retaliatory measures. One might think of such immunities as analogous to National Security Letters, now offered to reassure service providers that they can safely cooperate with government requests for information about Internet use patterns of private subscribers. Perhaps a better analogy is with the power to deputize private volunteers who assist law enforcement in special emergencies. Such deputies are immunized for some actions, relating to official assistance, but not for everything they may do.

Just as malicious attackers are able to take over end-user machines, researchers are sometimes able to infiltrate networks of compromised machines used by criminals. In some cases, researchers are able to seize control of these networks. One could imagine a team of white-hat hackers, seizing control of criminal-operated botnets and then cleaning up the damage behind them. Such action would violate laws against unauthorized access to computer systems,


210 See 18 USC § 2709. For relevant history and dispute about secrecy requirement, see Doe v Ashcroft, 334 F Supp 2d 471 (SDNY 2004); for acquiescence in light of subsequent legislation, see Doe v Gonzales, 449 F3d 415 (2d Gr 2006).

211 See, for example, Williams v US, 341 US 97 (1951) and Logar v Edmundson Oil Co, 457 US 922 (1982), both authorizing claims against private parties under 42 USC § 1983 for deprivation of rights “under color of state law,” when the private action was entangled with state authority. But commentators worry that many sorts of private “enforcement” action have been exempted from restrictions on government, such as Fourth Amendment search limits. See generally David Sklansky, Private Police, 46 UCLA L Rev 1165 (1999), Jon Michaels, Deputizing Homeland Security, 88 Tex L Rev 1435 (2010).

since the owners never gave permission for this sort of vigilante action.\textsuperscript{213} Such tactics also risk damaging the computers they are designed to protect. As a result, companies that might otherwise do so are now very reluctant to embrace such measures. But we might want to encourage researchers to develop such techniques—especially where government officials had given approval for their exercise.

It would be worthwhile to think about incentives for cooperation in such ventures. The government might offer financial rewards. It might even offer some analogue to "prize"—rewarding companies that assist in counter-measures by letting them claim ownership of website addresses or other assets seized from cyber criminals.\textsuperscript{214}

A second response would be to clarify, within federal law, that there is a right of self-defense against cyber attacks. New legislation might indicate what sort of countermeasures would fall within this right. It might also clarify what sorts of damages might be claimed in lawsuits when such limits have been exceeded. Such statutory provisions could reassure companies contemplating retaliatory measures. Companies that have seen foreign predators steal sensitive technical secrets through cyber intrusion might not need much encouragement to explore means of countering such intrusions through cyber counter-measures. But they would be more likely to act if more confident of their legal rights in taking such actions—and apprised in advance of legal limits on such actions.

All these measures—and the objections to them—could apply in a high-intensity cyber conflict as much as they do in the pervasive, low-level computer security challenges we already face. Just as authorizing privateers and armed merchant ships helped mobilize non-government resources in naval conflict, government authorization, qualified immunity, and reward would shift the balance in a cyber conflict. But as noted in Section IV, one of the main purposes of authorizing privateers was to impose costs on adversaries short of committing to all-out war.\textsuperscript{215} We would forego the tactical advantages of cyber retaliation if we regarded it solely as an adjunct to actual shooting wars with real bullets.

\begin{footnotes}
\item[213] 18 USC § 1030(a)(2(C) imposes criminal liability on anyone who “intentionally accesses a computer without authorization . . . and thereby obtains . . . information from any protected computer.”
\item[215] See text accompanying notes 118–126.
\end{footnotes}
A third legal reform to regulate cyber-conflict might be a fund to compensate third parties injured by government cyber attacks passing through foreign countries. In Iraq, the Pentagon developed a system of compensating families for accidental damage to private homes and property and for loss of life to relatives. The system has since been applied as well in Afghanistan. It has proved quite helpful in soothing local rage at "collateral damage." It is not a tort scheme, which acknowledges precisely defined legal rights. Much is left, it seems, to the discretion of local commanders, though larger claims must be approved by the theater commander. There is no provision for judicial review.

A cyber compensation fund might operate along somewhat similar lines. Here, too, it would probably be appropriate to operate the compensation fund separately from the court system. There might be conditions and restrictions—such as a promise not to reveal details of the attack. There are obvious reasons to limit legal formalities. But it could be helpful to have decisions of authorities reported and collected as an initial guide to what the United States regards as lawful retaliation and what it regards as a regrettable mistake—or an unsupportable excess.

VIII. CONCLUSION: CYBER NORMS WON’T COME FROM TREATIES

At the extreme, a cyber attack might produce catastrophic effects. A determined enemy might, for example, devise a cyber offensive which disabled the electric power grid of a target state for an extended period. In a full-scale conflict, a blow of that kind might have strategic effect, but also cause vast suffering. Without rail service or reliable refrigeration, portions of the civilian population might be exposed to extreme food shortages, even to the spread of epidemic diseases. A long line of commentators has, accordingly, warned that cyber weapons might prove so devastating to civilians that their use should be constrained by formal international agreements.
Other commentators have argued that with all their potential for catastrophic harm to civilians, cyber attacks would not likely secure decisive results in military terms. No first strike could hope to knock out the target state's capacity to retaliate, even in the cyber realm. Nor could the state that absorbed an initial cyber strike hope to eliminate the attacker's capacity to launch further cyber strikes. Some analysts conclude, therefore, that the most sensible course would be to head off a costly and futile arms race in cyberspace by negotiating formal agreements never to deploy cyber attacks for military purposes.\footnote{219}

If international diplomats could negotiate a reliable treaty barrier to cyber attacks, we would not have to think any further about offensive operations in the cyber realm. We would certainly not need to think about appropriate legal limits on cyber attacks and how to enforce them. A reliable treaty prohibition would certainly solve a great many problems—if we could achieve a reliable treaty. But is that alternative at all realistic?

Alas, in the world as it is, that happy solution seems as unlikely as putting our reliance in a treaty that prohibited all resort to military force.\footnote{220} Even if it were desirable to prohibit all recourse to cyber weapons by international agreement, such a treaty may not be obtainable. The states most likely to engage in destructive cyber attacks may not be willing to renounce their capacity to do so. Or they may demand conditions for participation in such a treaty that the United States could not accept.\footnote{221} No matter how extreme one's vision of all-out

\footnote{219} For one of the most recent versions of this argument, see Bruce Schneier, An International Cyberwar Treaty Is the Only Way to Stem the Threat, US News Opinion (June 8, 2012), online at http://www.schneier.com/blog/archives/2012/06/cyberwar_treati.html (visited Mar 4, 2013).

\footnote{220} It is customary, in arguments of this kind, to invoke the ill-fated Kellogg-Briand Pact of 1928, which purported to outlaw war. Kellogg-Briand Pact, 46 Star 2343 (1928). It is more in point to notice that Secretary of State Kellogg circulated a reassuring cover letter with the treaty, indicating that military action in self-defense would, of course, still be lawful. “There is nothing in the . . . treaty which restricts or impairs in any way the right of self-defence. That right is inherent in every sovereign.” Letter to Austen Chamberlain (British Foreign Minister) of June 23, 1928, reprinted in J.W. Wheeler-Bennet, ed, Information on the Renunciation of War 141 (Kennikat 1973). What made the treaty so useless was not that its object was utopian—curbing recourse to war for routine disputes—but that it could not establish an agreed definition of the crucial concept of “self-defense.” As a practical matter, the UN Charter has not done better.

\footnote{221} A problem emphasized in Christopher A. Ford, The Trouble with Cyber Arms Controls, 29 The New Atlantis 52 (2010) and Jack Goldsmith, Cybersecurity Treaties: A Skeptical View (Hoover Institution Future Challenges Essay 2011) (both noting that Russia, China and other countries view...
cyber war, it could hardly be as horrifyingly destructive as a war fought with nuclear weapons. Appeals to abolish atomic weapons started soon after the first use of such weapons in August of 1945. Yet there is not, even now, a treaty that prohibits use of nuclear weapons.

Another difficulty is illustrated by our experience with U-boats, the weapon that provoked most rage and anguish (at least on the Allied side) in the First World War. As noted in Section III, the Washington Naval Treaty of 1922 prohibited unannounced submarine attacks on civilian shipping. The prohibition was reaffirmed in the 1936 London Protocol. And it was completely disregarded by Germany from the first day of the next world war. An agreement that won’t be honored can be worse than useless if its delusional assurances are trusted to substitute for more reliable measures.

Yet cyber weapons would be even harder to regulate than submarines or nuclear weapons. It was not possible to build a fleet of submarines in secret, even with the more limited surveillance capacities available in the 1930s. It is not possible today to attain an arsenal of nuclear weapons without detection. It is a plausible hope that arms control agreements can limit acquisition or proliferation of such weapons. It is not plausible to think that international agreements, even supplemented with inspection programs, can stop hostile states from developing the capacity to undertake destructive cyber attacks.

The equipment required for planning and developing (or even launching) cyber attacks is not distinguishable from computer equipment used for entirely innocent purposes. That equipment is so widely distributed in a modern state that it would be impossible to verify the actual use to which every computer was devoted. It would be difficult to persuade any major power to forego development of cyber weapons when it has no means to verify that potential enemies were actually adhering to the same policy. Even if some powers were prepared to abstain from developing cyber weapons in this situation to show their good faith, their trust might be abused. In a world where some powers have the capacity to deploy devastating weapons and others do not, the temptation to resort to such weapons will likely be higher than in a world where the same capacities are available to all powers.

There is a still stronger reason to doubt the efficacy of treaty limitations in this area, however. It is that cyber attacks remain quite different from nuclear weapons or even submarine attacks. Nuclear weapons are so fearful that no state

has dared to use one since the initial use of these weapons in 1945. Even submarine attacks still produce such shudders that they have only been unloosed amidst full-scale war. In wars since 1945, only opposing warships have actually been attacked. Surprise submarine attacks on civilian shipping—especially when they are likely to cause large numbers of fatalities—have been almost unknown in the limited wars we have seen since 1945.²²³

By contrast, cyber attacks are already pervasive, because they can be used for spying and harassment, for theft and intimidation—for intrusions far below the level of “armed attack” that would clearly justify a military response with conventional weapons. The very flexibility of cyber strikes, however, makes them quite hard to regulate. Enemies have already seen that we will tolerate quite a lot of probing, harassing and looting from foreign hackers.

So, even if we surmounted all the political obstacles to negotiating a treaty against cyber attacks, we might have great difficulty enforcing such a treaty. Opposing powers would always be tempted to test the limits of the treaty with small-scale harassing attacks or by encouraging (while disclaiming responsibility for) attacks by criminal hackers or non-state “hacktivists.” We might have no way of proving these violations without releasing sensitive intelligence information to support our claims—thereby, in effect, rewarding violations and encouraging more of them.

If we want to maintain legal limits, it might be much more profitable to start from the other direction. Rather than asking what we would like to prohibit, we might better focus on what we are prepared to retaliate against and then think more concretely about what retaliatory actions would be appropriate. Current US policy seems to offer vague threats of possible military responses to extreme cyber attacks—without drawing clear lines to define unacceptable threats and without saying what response we might make to lesser (but still costly) cyber incursions.

One way to promote new standards would be to announce, very publicly, what sorts of response might follow what sorts of provocations. If we piously assert that cyber retaliation should never be used against “civilian objects,” we are proclaiming an ideal that won’t be taken seriously. Cyber attacks already strike civilian objects—routinely and pervasively. The challenge is to signal our readiness to retaliate for sufficiently damaging attacks, without making idle threats.

²²³ Attacks on civilian shipping occasioned much concern during the Iran-Iraq War in the 1980s but both sides relied on mines and aircraft rather than submarines. During the Falklands War, even the Royal Navy’s sinking of an Argentine warship, General Belgrano, provoked controversy because the attack (by submarine) occurred outside the immediate domain of military operations. For analysis of both episodes, see L.F.E. Goldie, Maritime War Zones and Exclusion Zones, in Robertson, ed, The Law of Naval Operations, 64 Intl L Studies 156, 171–77 (cited in note 156).
At present, we are warning hostile states against massive cyber attacks while tolerating pervasive attacks from private (or ostensibly private) predators. It is as if we had warned foreign navies against attacking our sea-borne commerce, but shrugged off attacks launched by pirates. Even President Jefferson, avowed skeptic toward investment in naval power, preferred to send Marines "to the shores of Tripoli" to deal with pirate attacks on American shipping in the Mediterranean. When we fail to respond to lesser challenges, we risk signaling irresolution in facing more daunting challenges. If we fail to face down cyber predators, we encourage more destructive cyber attacks from hostile states.

The most likely threat is not an all-out war in which cyber weapons are deployed, along with bombs and missiles and torpedoes at sea. The far more likely use of cyber weapons would be in pressure tactics in the border regions between war and peace. But the same resort may apply in either case.

Historically, limits on methods of war have been enforced by reprisal—that is, by retaliatory action from the injured party. That was how the "customs" of war developed, long before any formal treaties. The notion that limits can be enforced without reprisal is a recent conceit—an idea favored by the Red Cross but not embraced by states seriously contemplating military actions. Historically, it was precisely the states most engaged in armed conflict that shaped the limitations on such conflict. Rules of war at sea were determined by the major sea powers. And a sufficient number of rights and restraints were settled that their exposition took up large chunks of standard international law treatises, down to the early twentieth century.

What matters most in the cyber realm is what states with the capacity to retaliate will treat as acceptable—and what they are determined to counter with active reprisals. If we want to deter, we should offer more clarity about what we regard as so unacceptable that it requires a response. Abstract denunciations will

224 Joseph Wheelan, Jefferson's War, America's First War on Terror, 1801–1805 3, 40–54 (Caroll & Graf 2003), offers the most recent and detailed account of Jefferson's war on the Barbary pirates, noting that despite his reputation as "the most pacific" of the founders, Jefferson had advocated military action against the pirates as far back as the mid-1780s, when he became aware of the challenge as ambassador to France.

Navigating Conflicts in Cyberspace

speak less persuasively than concrete deeds. We should demonstrate what we regard as unacceptable by refusing to accept it—and demonstrating our rejection in a way that adequately impresses the perpetrator state.

Given the particular characteristics of cyber conflict, there may be no serious alternative. The alternative to reprisal in land warfare is supposed to be prosecution before international tribunals. The institution designed to answer to this vision, the ICC, has completed only one prosecution since it began operation in 2002.\textsuperscript{226} The states known to be most active in developing cyber attack capabilities—Russia, China, Iran, and North Korea—have (like the United States) declined to subject themselves to the ICC's jurisdiction. Even if the Court's jurisdiction could be established, it would, in most cases, face tremendous obstacles in trying to hold governments accountable for cyber attacks. Such attacks could easily be perpetrated by shadowy groups, operating through a chain of intermediaries in several different countries.

There is another reason why cyber conflict would not be easily constrained by formal treaty standards. In practice, many details regarding the definition of offenses or the standards of attribution would turn on technical arrangements subject to continual adaptation—particularly in the course of a more active conflict, when governments on both sides might resort to new tactics. So diplomats might spend a decade negotiating a treaty to manage or protect some particular piece of technical infrastructure and then find that crucial details had become quite obsolete by the time the treaty had been ratified.

One does not need to embrace the illusion that cyber war can be perfectly or neatly regulated to see that some restraining norms may be reinforced in the way laws of war have traditionally developed—by accretion of precedents, as belligerents signal limits they can accept and limits they will enforce by reprisal. We will develop more clarity about standards, if we are more open about our intentions as about our actual measures. Some claims may be resisted, some retaliatory measures denounced. Some threats may be withdrawn, some measures repudiated in consequence. But we have more hope of developing international respect for limits if we demonstrate that we are serious about enforcing limits.

The issue is not whether to seek clarifying and stabilizing norms or acquiesce to utter chaos in cyberspace. The issue is whether to prepare ourselves to enforce limits we can hope to maintain—or dream of limits that will magically

\textsuperscript{226} The ICC issued its first verdict on March 14, 2012 (Prosecutor v. Thomas Lubanga Dyilo). Only six other cases had reached the trial stage. The court had issued 22 arrest warrants by then, but had only been able to take six defendants into custody. All the pending cases involved countries in Africa. See International Criminal Court 10-Year Anniversary Website, About the Court, online at http://www.10a.icc-cpi.info/index.php/en/about (visited May 27, 2013).
enforce themselves. The choice is to treat cyber threats in the manner of previous military threats—or hope that enemies with the capacity and desire to inflict harm in cyberspace will be restrained by the moral force of admonitions from the Red Cross in Geneva.

The prospects for gradually developing some consensual limits are far more promising than the prospects for a comprehensive treaty. Formal limitations on war measures tended, in the past, to appear after wars, responding to lessons learned in wartime. The Geneva conventions negotiated after the Second World War were notably more cautious than the Hague Conventions negotiated before the First World War, let alone the interwar agreements on submarine warfare.

We have reasons to hope that the commercial importance of the Internet will encourage restraint. It should encourage governments to formulate restraints in rules or standards or at least rough norms. We have every reason to fear that a comprehensive treaty, negotiated before we have any experience with the full range of dangers and temptations associated with cyber conflict, will prove an escapist fantasy.