For New Challenges, Revisit Old Rules: Cyber Attacks and the Law of Armed Conflict

By Jeremy Rabkin[1] and Ariel Rabkin[2]

"'Chinese metaphysics . . . An abstruse subject I should conceive,' said Mr. Pickwick.

'Very, Sir,' responded Pott … [the writer] read up for the subject at my desire in the Encyclopedia Britannica*.'*

Indeed!' said Mr. Pickwick. I was not aware that that valuable work contained any information respecting Chinese metaphysics.'

'He read, Sir,' rejoined Pott … with a smile of intellectual superiority, 'he read for metaphysics under the letter M and for China under the letter C; and combined his information, Sir."[3]

"There are no new problems in the law, only forgotten solutions and the issues which arose yesterday will always arise again tomorrow."[4]

I. Introduction

In the summer of 2011, Gen. 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 O.K. to attack me, and I'm not going to do anything other than improve my defenses every time you attack me, it's very

[1] Professor of Law, George Mason University; PhD, Political Science, Harvard University

[2] Post-Doctoral Researcher, Department of Computer Science, Princeton University; PhD, Computer Science, University of California, Berkley

[3] CHARLES DICKENS, THE PICKWICK PAPERS, Ch. 51 (Oxford, 1898), p. 646 (first edition, 1837)

[4] EVAN J. WALLACH, *Partisans, Pirates and Pancho Villa: How International and National Law Handled Non-State Fighters in the 'Good Old Days' Before 1949 and That Approach's Applicability to the "War on Terror,"* 24 EMORY INT'L. L. REV. 549 (2010) at 552.

difficult to come up with a deterrent strategy."[5] At the time, there was much dispute about whether the United States could use cyber technology as an offensive weapon and 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."*[6]

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.[7] A customized computer virus, devised by American specialists, had somehow been introduced into the equipment regulating Iranian centrifuges, causing the

---

[5] Thom Shanker and Elizabeth Bumiller *, Hackers Gained Access to Sensitive Military Files,* THE NEW YORK TIMES, July 14, 2011

[6] Sec. 954. The Conference Report (H. Rept. 112-329), CONGRESSIONAL RECORD, Vol. 157, No. 190 (Dec. 12, 2011) for this section of the bill explains that the original House bill sought to "clarify that the Secretary of Defense has the authority to conduct clandestine cyberspace activities in support of military operations … outside the United States or to defend against a cyber attack on an asset of the Department of Defense." The report then seems to undermine the restrictive proviso regarding laws of armed conflict and the War Powers Resolution: "The conferees recognize that in certain instances, the most effective way to deal with threats and protect U.S. and coalition forces is to undertake offensive military cyber activities, including where the role of the United States Government is not apparent or to be acknowledged." There would be no need for such concealment if cyber attacks were undertaken as part of larger war measures, already publicly avowed – and they would be hard to keep secret (as to their source), if Congress had already authorized military action under the War Powers Resolution or received formal presidential notification of impending attacks, as the WPR requires.

[7] David Sanger, *Obama ordered sped up wave of cyberattacks against Iran*, THE NEW YORK TIMES, June 1, 2012

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 – 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. 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 might be called "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.

In September of 2012, the Legal Adviser to the State Department, Harold Koh, spoke at an inter-agency conference hosted by U.S. 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

[8] Harold Hongju Koh, Legal Adviser, *International Law in Cyberspace*, Remarks at USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD Sept. 18, 2012 transcript available at http://www.state.gov/s/l/releases/remarks/197924.htm

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 U.S. 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 U.S. 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.

So official policy seems to regard cyber weapons as subject to the law of armed conflict but actual practice remains quite murky and obscure. At least some of the hesitation to clarify American policy seems to reflect enduring concerns about international legal standards. Some months before Koh's address, Stewart Baker, former general counsel to the National Security Agency (and former Assistant

---

[9] Office of the National Counterintelligence Executive, FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE, 2009-2011, Oct. 2011; The White House, STRATEGY TO COMBAT TRANSNATIONAL ORGANIZED CRIME*:* ADDRESSING CONVERGING THREATS TO NATIONAL SECURITY, July 2011.

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 …."[10]

If U.S. officials 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 to the Geneva Conventions (1977), apply in full to cyber conflict.[11] A long line of commentators embraces the same view.[12]

But most commentators seem to 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 (Red Cross version). They add to their sources 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."

---

[10] Stewart Baker, *Denial of Service, Lawyers are crippling America's abilty to defend against cyberwar with arcane rules and regulations*, FOREIGN POLICY, Sept. 30, 2011.

[11] International Committee of the Red Cross, "Cyber warfare, 29-10-2010 Overview," available on ICRC website: www.icrc.org, at p. 1.

[12] See e.g., Richard W. Aldrich, *The International Legal Implications of Information Warfare*, AIRPOWER J. (Fall 1996), pp. 102-106 (same principles apply); Department of Defense, Office of General Counsel, *An Assessment of International Legal Issues in Information Operations*, May 1999, esp. p. 8 ("Purely civilian infrastructures must not be attacked unless the attacking force can demonstrate definite military advantage"); THOMAS C. WINGFIELD, THE LAW OF INFORMATION CONFLICT, NATIONAL SECURITY LAW IN CYBER SPACE (2000), esp'ly pp. 44-46, summarizing conventional wisdom of 1990s; Eric Talbot Jensen, *Unexpected Consequences from the Knock-on Effects: A Different Standard for Computer Network Operations?* 18 AM. U. INT'L. L. REV. 1145 (2003) (answering title question in the negative); and most recently, Oona Hathaway, et al., *The Law of Cyber-Attack,* 100 CAL. L. REV. 817 (2012), esp. at pp. 851-54.

We do not argue that cyber space should be regarded as a law-free zone. We emphatically do not argue that cyber attacks can be deployed without any regard to legal limits on their effects. Instead, we argue that it would be more appropriate to ground American 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 body of law extended into more ambitious constraints in very recent times by advocates of the Red Cross view of armed conflict.

In the next section, we offer a general survey of ways in which war at sea has arrived at 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 Sec. III, we apply this analogy to questions about when it is proper to resort to force when the "force" is a cyber attack. In Sec. IV, we apply the analogy to analyze proper targets in cyber space and in Sec. V, proper participants. Sec. VI 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. Sec. VII 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. The Analogy of War 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.[13] 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 the claims of neutral shipping – a concern closely analogous to one of the central concerns about cyber conflict.

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.[14]

---

[13] For example, Duncan Hollis, *An e-SOS for Cyberspace*, HARV. J. INT'L. L.. (Summer 2011) at pp. 412-414; George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT'L. L. 1079 (Nov. 2000) at pp. 17-19

[14] 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." YVES SANDOZ et. al., COMMENTARY ON ADDITIONAL PROTOCOLS (1987), p. 598, par. 1863. The earliest source cited in support of this claim is the 1864 "St. Petersburg Declaration" which stipulated that "the only legitimate objective which States endeavor to accomplish during war is to weaken the military forces of the enemy." 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.

The background impulse is often described as "humanitarian" – seeking to avoid unnecessary suffering, particularly to innocents. But that is a wider (and distinguishable concern) than the principle of "distinction."[15] In war on land, there were also practical reasons for such restraint. In war on land, the usual object 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 – in contrast to the developing trend in land warfare by the Eighteenth Century – naval war never exempted civilian property. 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.

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

[15] See, .e.g., GARY SOLIS, THE LAW OF ARMED CONFLICT (2010), pp. 250-57, 269-71, which sets out "distinction" as one of "four core principles" in its overview, then discusses avoiding "unnecessary suffering" as a separate "core principle." Similarly, GEOFFREY CORN, VICTOR HANSEN, et al., THE LAW OF ARMED CONFLICT: AN OPERATIONAL APPROACH (2011) identifies "Military Necessity" and "Humanity" as "Cardinal Principles," then discusses "Distinction" and "Proportionality" as "Implementation Principles" (pp. 115 - 124). The Hague Convention on Law and Custom of War on Land (1907 - 205 C.T.S. 227), the classic early source, prohibited signatories to "employ arms, projectiles or material calculated to cause unnecessary suffering" (Annex: Art. 23e) – without limiting the prohibition to weapons affecting civilians. That convention did not even use the term "civilian" (except in one provision – Annex: Art. 29 – dealing with "soldiers and civilians … intrusted [sic] with 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 16th Century but the OXFORD ENGLISH DICTIONARY records no use of the term "civilian" – in the sense of non-military – until the late 18th 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.

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.[16]

The provision in the U.S. Constitution, authorizing Congress to issue "letters of marque and reprisal," reflects the traditional practice of targeting enemy commerce. Letters of marque could increase the naval capacity of a country with few actual warships. Letters of marque 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. 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.[17] 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 attack

---

[16] For historical overview, John Hattendorf, *Maritime Conflict* in MICHAEL HOWARD, ed., THE LAWS OF WAR, CONSTRAINTS ON WARFARE IN THE WESTERN WORLD (1994), esp. pp.103-113

[17] WILLIAM C. DAVIS, THE PRIATES LAFITTE, THE TREACHEROUS WORLD OF THE CORSAIRS OF THE GULF (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 U.S. government to prey on Spanish commerce.

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.[18]

Letters of marque, still an important part of U.S. 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.[19] Commentators in the

---

[18] Theodore Cooperstein, *Letters of Marque and Reprisal: The Constitutional Law and Practice of Privateering,* 40 J. MAR. L. & COM. 221 (2009) reviews colonial practice and experience under the Articles of Confederation (during the War of Independence), which confirmed for the Framers the military value of the system.

[19] "… the 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." LASA OPPENHEIM, INTERNATIONAL LAW (2d. ed., 1912), Vol. II, §178, p. 222.

early Twentieth Century noted that as other powers built formidable navies, they also came to resist restrictions on naval warfare.[20]

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 territory. 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 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.[21] Even viewed from this perspective, however, the experience of war at sea offers many instructive analogies.

---

[20] "Since the growth of navies among continental Powers, these Powers have learnt to appreciate the value of the rule in war [allowing capture of enemy merchant ships] 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 the 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., p. 223

[21] See Note 15, supra. 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. (http://www.icrc.org/ihl.nsf/INTRO/110?OpenDocument). The Code prohibits "the wanton devastation of a district" (Art. 16) and admonishes that "the unarmed citizen is to be spared in person, property, and honor as much as the exigencies of war will admit." (Art. 22) It nonetheless approves "all destruction of property and obstruction of the ways and channels of traffic, travel or communication" (Art. 15) and holds it "lawful to starve the hostile belligerent, armed or unarmed, so that it leads to the speedier subjection of the enemy." (Art. 17)

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."[22]

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. But in a larger view, the experience teaches something about the enduring importance of humanitarian restraint.

At the outbreak of war in 1914, Britain and France sought to blockade German ports and then sought to prevent shipping of contraband to neighboring ports (from which cargoes could be brought overland to Germany or its allies). Germany announced a countering exclusion zone around the British Isles. As most of its own surface fleet was held in check by superior Allied surface fleets, Germany asserted the right to enforce its exclusion policy with submarine attacks on all shipping in the prohibited area. The new term "economic warfare" came into use to describe these measures, which seemed to be much more encompassing than

[22] JOHN KEEGAN, THE PRICE OF ADMIRALTY: EVOLUTION OF NAVAL WARFARE (1988), pp. 91-92, describing efforts of Royal Navy ships to save prize ship crews, even at risk to themselves.

blockades in earlier wars, which had focused on closing specific ports or blocking imports of militarily related "contraband."[23]

If their strategic logic was comparable, these tactics did not operate the same way in practice. Allied blockade measures were enforced with surface war ships, which could either divert merchant ships or demand that they submit to be taken as prize. Submarines could not divert crews to take direct control of the merchant ships they tried to stop. In practice, submarines could not even safely approach a merchant ship if the latter were prepared to defend itself. Submarines were lightly armed. Their thin hulls made them very vulnerable, even to small gauge guns. So submarines often attacked without warning. When they managed to sink a ship, they could do little to rescue survivors. Submarine warfare therefore looked like sheer slaughter on the seas, extending not only to naval crews but to civilians.[24]

Attacks without warning provoked immense indignation, particularly when the victims were neutrals.[25] The sinking of the British passenger liner Lusitania in

---

[23] DAVID STEVENSON, CATACLYSM, THE FIRST WORLD WAR AS POLITICAL TRAGEDY (2004), p. 201

[24] ". . . 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 ship-owners 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." PAUL HALPERN, A NAVAL HISTORY OF THE FIRST WORLD WAR (1994), pp. 291-92

[25] 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." See 11 AM. SOC'Y. INT'L. L. PROC. 11 April 26-28, 1917 (Address by Charles Cheney Hyde at 31; Remarks of Everett Wheeler at 36)

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 resumption of such attacks in 1917, it provoked American entry into the war on the Allied side.[26]

Allied indignation was still so strong after the war that Britain demanded a total ban on submarines and a rule that commanders who ordered attacks on civilian shipping without warning should be treated as pirates. 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. The 1936 agreement on submarine warfare reemphasized the restriction and Germany was among the states that agreed to these terms.[27]

Nonetheless, at the outset of the Second World War, Germany immediately resumed the practice of submarine attacks without warning. Britain and then the United States copied the tactic in their own war efforts (though the Allies did not attack neutral shipping). After the war, the Nuremberg Tribunal refused to impose punishment on Admiral Karl Doenitz, commander of the German U-boat force, for sinking civilian ships without warning. The Tribunal noted that Allied navies had engaged in a similar practice, so it no longer seemed to be recognized as a tactic prohibited by international law. The Tribunal still found that, even in an all-out war, some humanitarian restraints should have been respected. Admiral Doenitz was

---

[26] "Unrestricted submarine warfare was an essential cause of American entry [into the World War] and not simply a pretext for it." STEVENSON, CATACLYSM, p. 261

[27] For debates in the inter-war period, see Howard S. Levie, *Submarine Warfare: With Emphasis on the 1936 London Protocol,* in Richard Grunawalt, ed., THE LAW OF NAVAL WARFARE: TARGETING ENEMY MERCHANT SHIPPING, 65 INT'L. L. STUD. (1993)

sentenced to twenty years in prison for ordering his U-boats to fire on ship-wrecked crews, struggling in the water after their ships had been torpedoed.[28]

Allied indignation against indiscriminate attacks by U-boats is all the more notable because the Allies were simultaneously applying much pressure 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 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.[29]

Again, the analogy with cyber conflict is very clear. Cyber attacks can disable equipment and cause considerable economic damage, without causing direct injury 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 or unavoidable. Cyber attackers can choose to keep attacks below that level and will often have definite incentives to do so. Even below that threshold, 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

[28] TELFORD TAYLOR, THE ANATOMY OF THE NUREMBERG TRIALS (1992), pp. 399-409

[29] The distinction was still compelling to some scholars decades later: Robert W. Tucker, *The Law of War and Neutrality at Sea*, 50 INT'L. L. STUD. 140 (1957) at p. 278

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.[30]

The experience of war at sea in the world wars 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 the narrowest legal terms. For the debate about submarine tactics in the world wars was partly driven by another, less noted innovation. Britain, on the eve of the First World War, announced that it would place guns on some of its merchant ships. The British insisted that the guns were only for defensive purposes.[31]

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 do so against suspected 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

[30] 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 especially 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 (2000), provides many examples (as at 46-47, Iraq; 73-74, Serbia). BRUNO SIMMA et al., CHARTER OF THE UNITED NATIONS (2d ed., 2002) reports concerns of Security Council members to avoid "negative humanitarian consequences as much as possible" – without at all limiting economic sanctions solely to military activities in the target state.

[31] Levie, *Submarine War*, at 37-38, notes 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.

uncertainty among submarine commanders about which ships could safely be given advance warning.[32]

The Germans protested that the arming of civilian ships was essentially a return to privateering, hence a violation of the Declaration of Paris. In 1916, German authorities executed the captain of an armed British merchant ship for having engaged in sea combat as a civilian – hence, in the German view, engaged in conduct equivalent to piracy.[33] A leading British legal commentator had acknowledged, before the war, that international law would regard merchant crews as pirates if they engaged in armed conflict, even with enemy warships, while otherwise failing to abide by rules applicable to warships.[34]

The problem for the British was that, if armed merchant ships were viewed as warships, there was no rule against an enemy attacking them without warning. But it would be a violation for neutrals to accept them into their ports for more than 24 hours, the limit specified for warships in the 1907 Hague Convention on the duties of neutrals. If merchant ships stayed longer, they would compromise the obligation of neutrals not to provide bases for belligerent warships in the midst of a

[32] 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." THE WORLD CRISIS (1939) Vol. II (Pt. III, Ch. 15), p. 1226

[33] HALPERN, NAVAL HISTORY, p. 196

[34] OPPENHEIM, INTERNATIONAL LAW (1912), Vol. II, §181, p. 226, 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."

conflict. One day was rarely enough time, however, for a merchant ship to unload its cargo and take on a new cargo for its subsequent voyage.[35]

The Germans thus had serious legal grounds to protest 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.[36] But 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.[37] The United States adopted the practice itself in 1917 – even before it entered the war.[38] In the 1930s, advocates of isolation in the United States insisted that arming American merchant ships – and receiving armed British merchant ships

---

[35] Levie, *Submarine Warfare*, p. 36, explaining implications of Hague Convention XIII (1907), Art. 12, Art. 24.

[36] German objections are surveyed in A. Pearce Higgins, *Armed Merchant Ships*, 8 AM. J. INT'L. L. 705 (1914) at 714-16; neutral concerns described in Levie, *Submarine Wafare* at 36.

[37] CHURCHILL, WORLD CRISIS, Vol. II (Pt. III, Ch. 15), p. 1229, reports that during 1916, "defensively armed" merchant ships escaped unharmed in 76 per cent of their encounters with U-boats (236 out of 310), whereas only 22 per cent of "unarmed ships" managed to escape such encounters (22 of 302), while the overwhelming majority of "unarmed ships" (235 of 302) were sunk. 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, HISTORY OF THE U.S. NAVY, 1775-1941 (1992), p. 481.

[38] President Wilson proposed the arming of U.S. 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. Relevant documents at 11 AM. J. INT'L. L. 350, 352 (1917). Congress amended the 1936 Neutrality Act to allow arming of U.S. merchant ships on Nov. 17, 1941 – three weeks before a formal declaration of war. The politics are described in S.E. MORISON, HISTORY OF U.S. NAVAL OPERATIONS IN WORLD WAR II, Vol. I (Battle of the Atlantic)(1975), pp. 296-97.

in American ports for extended stays – had compromised American neutrality and should not be repeated in the event of a future war.[39]

Yet, for all that, Britain again armed its warships at the outset of the Second World War. And in that war, too, American merchant ships were also armed, and armed again before the U.S., itself, became an official belligerent. The scale and speed of German aggression left fewer neutrals to protest by the time the United States did become a full belligerent power. But before that, neutral opinion, certainly in the United States, viewed the arming of merchantmen with indulgence while strongly condemning U-boat attacks. The former seemed to draw moral force 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.[40] U-boats attacks continued to be viewed as wanton, because immediate and inescapable, attacks on civilian life.

Here, too, there are obvious analogies with cyber conflict. The capacity to respond to cyber attacks is not limited to secret programs in government research facilities. Not only military facilities but the whole range of government agencies, civilian as well as military or defense-oriented, state and local as well as federal,

---

[39] Statement of Professor Edwin Borchard, 31 AM. SOC'Y. INT'L. L. PROC. 173 (1937): "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." Borchard held to the same view at the start of the next war: *Armed Merchantmen*, 34 AM. J. INT'L. L. 107 (1940)

[40] "A merchantman sailing the seas has a right to defend his property … There is the further right of self-preservation …." Chandler Anderson, "The Status of Armed Merchantmen," 11 AM. SOC'Y INT'L. L. 11 (April 26, 1917); As a French commentator 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 Pearce, DEFENSIVELY ARMED MERCHANT SHIPS, at p. 36

might be objects of attack in a cyber conflict. So might critical infrastructure – electric power grids, transportation networks, financial exchange mechanisms – on which the private economy depends. So might hundreds of thousands of firms in the private economy. 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 not be unthinkable.

Another lesson of naval war in the Twentieth Century is that great powers have the decisive say about the rules. In the early years of both world wars, British and French decision-makers worried a great deal about American reactions to their policies, especially on the high seas where American interests were most directly affected. 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 as well as by German U-boat tactics. 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, which could only be obtained by submitting to Allied inspectors in ports of embarkation, including even neutral parts. The system had no precedent in naval war but it suited the needs – and could be imposed by the massed strength – of Allied powers at sea.[41] Neutrals protested, but complied. The system threatened shipping rights (and

[41] HUGH RITCHIE, THE 'NAVICERT' SYSTEM DURING THE WORLD WAR (1938). 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 overland from there.

commercial opportunities) but did not threaten the lives of ship crews or passengers.

When powerful states feel pressed by circumstances, as in a long war, they are bound to give less weight to constraining rules and more attention to harnessing all their resources to immediate ends. 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 perfected and intensified it, causing hundreds of thousands of civilian casualties, along with 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. Allied governments did not want to acknowledge that their own wartime practices had been unlawful.[42] There were no general restraints on targeting in in the four Geneva Conventions negotiated in 1949.[43]

Very constraining limits did appear in Additional Protocol I to the Geneva Conventions (API I), negotiated at a new round of Geneva conferences in the mid-1970s, at which the Third World majority at the UN predominated. The effort 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

[42] TAYLOR, ANATOMY OF THE NUREMBERG TRIALS, pp. 325-27

[43] Convention I (75 UNTS 31) provides protections for "wounded and sick" combatants and medical personnel; Convention II (75 UNTS 85) provides parallel protections for "wounded, sick and shipwrecked" combatants at sea; Convention III (75 UNTS 135) sets out protections for "prisoners of war" in enemy captivity; only Convention IV (75 UNTS 287) covers protections for "civilians" – but limits its protection to persons already "in the hands of" 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.

powers – Turkey, Israel, India, Indonesia among others – also declined to ratify AP I. Leading NATO states (Britain, Canada, Germany, Italy) ratified only with important reservations (including refusal to embrace prohibitions on reprisals in kind against unlawful targeting).[44]

Almost all the limiting provisions in AP I did find their way into the Statute of the International Criminal Court, negotiated in 1998. Again, however, the United States and a considerable number of other powers (Russia, China, India, Pakistan, Israel, Egypt, Indonesia, etc) 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 the past decade have not often displayed close adherence to AP I standards.[45]

---

[44] Reservations by NATO states (and others) are conveniently summarized in ADAM ROBERTS AND RUICHARD GUELFF, eds. DOCUMENTS ON THE LAWS OF WAR (3d ed., 2002), p. 499-512. ELMAR RAUCH, PROTOCOL ADDITIONAL I TO THE GENEVA CONVENTIONS: *Repercussions on the War of Naval War* (Berlin, 1984), p. 161 et seq quotes extensively from comments of western delegates at the framing conference in Geneva in the mid-1970s, insisting that a right of reprisal must be allowed to enforce contemplated limits.

[45] Conflicts in central Africa have routinely involved attacks on civilians, even when armies have crossed an international border to reach them. International authorities have not devoted much attention to such episodes. Though the International Criminal Tribunal for the Former Yugoslavia insisted that AP I standards had, by the 1990s, become applicable even to domestic conflicts, Russia ignored these standards when it bombed civilian centers in Chechnya in 1995. It did not provoke any serious international condemnation. Russia continued to be treated, for example, as a member in good standing of the Council of Europe and a full participant in the European Convention on Human Rights. Indiscriminate rocket attacks directed at Israel from Gaza provoked ritual statements of disapproval from western capitals but no threat of action against the ruling authorities in Gaza. Only action by western nations – such as threatening to cut off aid or trade relations – could give force to AP I standards in such conflicts. Such action has never been threatened. The least one can say is that these standards are not considered universally obligatory. British authorities insisted that their military actions in Libya in the spring of 2011 were in full compliance with these standards. The standards may take priority when the only countering consideration is excess mortality among foreigners in a needlessly prolonged war. We do not know how faithful even western powers would be to these standards if they were fighting a war in which their own people were directly threatened.

Whatever one thinks of these developments, it remains notable that major naval powers – including a number of formal signatories to Additional Protocol I -- have declined to embrace AP I as a guide to permissible tactics in war at sea. Naval powers 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."[46] 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 contemporary humanitarian claims are more demanding than practice in the world wars. The Manual accordingly emphasizes a responsibility 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 most kinds of civilian cargo from going in or out of enemy ports. It also authorizes seizure of neutral ships to limit sea-borne supply to an enemy of cargo that "may be susceptible for use in armed conflict."[47]

---

[46] 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 (1995)

[47] Art. 148

The San Remo Manual thus offers a much more encompassing approach to permissible targets than that proclaimed in AP I, which limits attacks to objects "whose total or partial destruction … *in the circumstances ruling at the time*, offers a *definite* military advantage."[48] AP I is primarily concerned with attacks against "objects" on land. It seems to assume the targets are "objects" situated in enemy territory which must usually be attacked from a distance – by air strikes or artillery – so the effectual choice will 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 it to their own advantage.

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

[48] Art. 52, Par. 2 (emphasis added)

easily detected and not easily repaired.[49] That is what made the Stuxnet attack on the Iranian nuclear program so remarkable – that it continued to 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.[50]

As with naval powers, so with powers 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 on the seas in the age of pirates (and still is, to some degree). Pirates and terrorists do not need submarines and aircraft carriers to impose serious costs on seaborne commerce. Criminal gangs engage in hacking

---

[49] Marty Lyons, *Threat Assessment of Cyber Warfare* (University of Washington/Homeland Security, Dec. 2005) identifies ongoing offensive cyber programs in China, India, Iran, North Korea, Pakistan, Russia. Study available at: http://www.cs.washington.edu/education/courses/csep590/05au/whitepaper_turnin/Lyons-P590TU-White%20paper.pdf

[50] The success of this particular strike seems to have depended on close cooperation from Siemans, the German industrial firm that supplied equipment to the Iranian program. Not every attacker could expect to receive such assistance from a western manufacturer.

efforts to steal secrets, scam the gullible, extort protection payments from the vulnerable. As with pirates in earlier times[51] 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"[52] and limits the authority of warships to interfere with foreign shipping to a narrow set of circumstances, which do not include wartime tactics.[53] Still, the treaty includes a half dozen 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

---

[51] JENNIFER MARX, PIRATES AND PRIVATEERS OF THE CARIBBEAN (1992) describes the British government's connivance at attacks on Spanish commerce from the time of Francis Drake in the 16th Century until well into the 18th Century – with efforts to suppress unlicensed (entirely piratical) attacks "uneven at best, intensifying or not according to the questions of politics and economics" of the moment. (at 26)

[52] Art. 88, U.N. Convention on the Law of the Sea, completed Dec. 10, 1982 (21 I.L.M. 1261)

[53] Art. 110 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." Articles 101-107 specify other rights and responsibilities of warships in dealing with pirate ships. All other categories in Art. 110 are only covered in isolated, one-off provisions.

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.[54] 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 U.N. Security Council has revived the older approach, expressly (and repeatedly) authorizing the world's navies to fire on pirate ships that refuse to surrender.[55] 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.

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

[54] ALFRED P. RUBIN, THE LAW OF PIRACY (2006), pp. 221-225 (application of law of war to pirates)

[55] S.C. Res. 1816 (June 2, 2008); S.C. Res. 1838 (Oct. 7, 2008); S.C. Res. 1844 (Nov. 20, 2008); S.C. Res. 1846 (Dec. 2, 2008); S.C. Res. 1851 (Dec. 16, 2008)

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. 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 a weapon 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."[56] The warning – and the seemingly irresistible metaphor – was even embraced by the Director of Central Intelligence, shortly before he became Secretary of Defense.[57] 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 U.S. air traffic control system while hundreds of

[56] The phrase "cyber Pearl Harbor" is now deeply entrenched: a Google search of the phrase in November 2012 generated over 1.5 million results. Some prefer a more updated metaphor: NATO's chief of cyber defense claimed "cyber attacks pose as great a threat to national security as a missile attack." Kevin Coleman, *Cyber Weapons and E-Bombs*, DEFENSETECH.ORG, Mar. 13, 2008 (http://www.defensetech.org/archives/cat_cyberwarfare.html)

[57] Leon Panetta invoked the clichéd term in testimony before the Senate Armed Service Committee, during hearings on his nomination to the post of Defense Secretary (June 9, 2011), having served more than two years by then as Director of the CIA. For one account of the receptive reaction, see Anna Mulrine, *Panetta: The Next Pearl Harbor could be a cyber attack,* CHRISTIAN SCIENCE MONITOR, June 9, 2011.

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 "armed force." 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.[58] 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 U.S government computers to leave behind a taunting message, the equivalent of scrawling naughty words on the front fence.[59] No one would think it reasonable to respond to such a prank with cruise missile strikes. There would be formidable legal objections to deploying conventional force in retaliation for an "attack" that was no more than the cyber equivalent of an adolescent prank.

---

[58] A Russian military analyst has claimed that Russia "retains the right to use nuclear weapons first against the means and forces of information warfare and then against the aggressor State itself." V.I. Tsymbal, Address at the Russian-US Conference in Moscow, Evolving Post-Cold War National Security Issues, Sept. 12-14, 1995 (quoted in Timothy Thomas, *Russian Views on Information Based Warfare*, AIRPOWER J. Spec.Ed. 1996 at 25

[59] Hackers with a perverse sense of humor have played with the ambiguity of such "penetration." On June 14, 2011, the U.S. Senate's website was hacked by a group calling themselves "LulzSec," who posted this message: "This is a small, just-for-kicks release of some internal data from Senate.gov. Is this an act of war, gentleman?" Andrew Morse and Ian Sherr, *Senate Website Gets Hacked*, WALL ST. J. June 14, 2011.

The UN Charter obligates members to "settle their international disputes by peaceful means"[60] and to "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state."[61] The Charter gives broad powers of coercion to the Security Council[62] 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 self-defense when an armed attack occurs."[63]

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.[64] 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

[60] Art. 2, Par. 3

[61] Art. 2, Par. 4

[62] Art. 39-50

[63] Art. 51

[64] See, e.g., Michael Schmitt, *Computer Network Attack and the Use of Force in International Law*, 37 COL. J. TRANS'L. L. 885 (1999); Richard Aldrich, *How Do You Know You Are at War in the Information Age?* 22 HOUS. J. INT'L. L. 223 (1999-2000); Jason Barkham, *Information Warfare and International Law on the Use of Force,* N.Y.U. J. INT'L. & POL. (Fall 2001); Daniel B. Silver, *Computer Network Attack as a Use of Force under Article 2(4) of the UN Charter*, 76 INT'L. L. STUD. 73 (2002), p. 73; Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense,* 38 STAN. J. INT'L. L. 207 (2002); Thomas Wingfield, *When is a Cyber Attack an 'Armed Attack?"* (Paper distributed by Potomac Institute, 2006); Matthew Waxman, *Cyber Attacks as 'Force' under UN Charter Article 2(4*), 87 INT'L. L. STUD. (2011); Oona Hathaway et al., *The Law of Cyber-Attack* 100 CAL. L. REV. 817 (2012).

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."[65]

Trying to define the precise threshold where a cyber attack becomes an "armed attack" may be missing the main point, however. Many analysts have followed Air Force 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 that which would be associated with 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.[66]

Under whatever rubric, however, we still have to decide when and how to respond. The issue may seem legalistic but it is 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.[67] 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

---

[65] *Cyberwarfare is becoming scarier*, THE ECONOMIST, 24 May 2007; John Schwartz, *When Computers Attack*, THE NEW YORK TIMES, June 24, 2007; Gadi Evron, *Battling Botnets and Online Mobs,* GEO. J. INTL. AFF.

[66] The argument seems to have first been developed by Michael Schmitt *in Computer Network Attack and Int'l Law*, INT'L. L. STUD. (2002). Schmitt renewed the argument in "The Law of Targeting" in ELIZABETH WILMHURST and SUSAN BREAU, eds., PERSPECTIVES ON THE ICRC STUDY (2007), then again in Schmitt, *Cyber Operations and the Jus in Bello*, 87 INT'L. L. STUD. 89 (2011).

[67] See FN 48, supra.

contractors as well as other sensitive targets. They also seem to be encouraging criminal networks to develop their capacities.[68]

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.[69]

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 Art. 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 – those

---

[68] Office of National Counter-Intelligence Executive, Report, Nov. 2011 at: http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf
In world of cybertheft, U.S. names China, Russia as main culprits, WASHINGTON POST, Nov. 5, 2011
Ellen Nakashima and William Wan, "China's denials about cyberattacks undermined by video clip," *The Washington Post*, Aug. 24, 2011 (on video indicating state support for hacking operations directed at the U.S.)

[69] For one assessment, see HENRY KISSINGER, DIPLOMACY (1994), pp. 773-75 (emphasizing opposition to Soviet expansion, rather than support for democracy as an aim in itself, in explaining U.S. policy in Central America and elsewhere in the 1980s).

for which a full military response is required, as against those for which any forceful response is forbidden.

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 countering measures, culminating in deployment of the armed forces of the member states in full-scale combat operations.

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.[70] Such "measures … may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio and other means of communication …."[71] 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."

The Charter acknowledges a problem that challenged states long 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

[70] LELAND M. GOODRICH, EDVARD HAMBRO, ANNE P. SIMMONS, CHARTER OF THE UNITED NATIONS, *Commentary and Documents* (3rd rev. ed, 1969), surveys the deliberations at San Francisco regarding Art. 41 (pp. 311-314), reporting no concern that excessive sanctions might be improper or implicitly constrained by the Charter.

[71] Art. 41

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 in the previous section, the U.S 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 capture on land and water."[72] 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.[73]

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 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

[72] 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 in attacks on isolated manor houses – as well as capturing other ships on "water."

[73] C. Kevin Marshall, *Putting Privateers in Their Place: The Applicability of the Marque and Reprisal Clause to Undeclared Wars*, 64 U. CHI. L. REV. 953 (1997) argues even the President might authorize the practice in response to attacks by foreign naval forces – even without congressional authorization, let alone declaration of war.

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 U.S. 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. 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 of 1800.[74]

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.[75] Burlamaqui described "imperfect war" as one "which does not entirely interrupt the peace, but only in certain particulars, the public tranquility being in other respects

---

[74] ALEXANDER DeCONDE, THE QUASI-WAR: THE POLITICS AND DIPLOMACY OF THE UNDECLARED WAR WITH FRANCE, pp. 124-130 (1966)

[75] For example, James Wilson, one of the most influential delegates at the Philadelphia Convention and subsequently among the first justices of the U.S. Supreme Court, cited Burlamaqui with some regularity: The most recent edition of the COLLECTED WORKS OF JAMES WILSON (Kermit L. Hall and Mark David Hall, eds., 2007) contains 11 references to Burlamaqui in the index (compared with 12 references to Vattel, 17 to John Locke, 3 to J-J Rousseau).

undisturbed."[76] 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.[77] Was the liberation of the ship from French hands taking it "from the enemy" (as a 1799 statute required, for determining the compensation to the ship that made the "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 authorized" to attack certain objects, for certain purposes.[78]

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

[76] PRINCIPLES OF NATURAL AND POLITIC LAW, trans. By Thomas Nugent (Indianapolis: Liberty Fund, 2006, reprinting London edition of 1763), Part IV, Ch. 3, §331, p. 475. The original French edition was published in 1757.

[77] *Bas v. Tingy*, 4 Dall. 37 (1800)

[78] Id., at 46

"pacific reprisals."[79] A more systematic response was "pacific blockade," shutting a foreign port in peacetime as a way of applying economic pressure on the targeted state.[80]

Well into the Twentieth Century, naval deployments were used to intimidate a target state without necessarily committing to land invasion – hence the expressive term "gun boat 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.[81] The challenge has endured, despite 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,

[79] See, e.g., OPPENHEIM, INTERNATIONAL LAW: "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." Vol. II, §42, p. 47. 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." (§37, p. 41) The term "pacific reprisals" does not imply absence of force or violence but the absence of a surrounding context of war, as would be true for "belligerent reprisals." For endorsement of such peacetimes ventures in limited military strikes for purpose of retaliation, see Michael Newton, *Reconsidering Reprisals*, 2010 DUKE J. COMP. & INT'L. LAW 61 (Spring 2010)

[80] Id., Vol. II, §48-49, pp. 48-53

[81] J. CABLE, GUNBOAT DIPLOMACY, 1919-1991: POLITICAL APPLICATIONS OF LIMITED NAVAL FORCE (3d ed., 1994), which 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." (at 14) The list of episodes (pp. 157-213) purports to be illustrative rather than exhaustive. Of these episodes, 89 (more than one third) involved the U.S. Navy, though often in joint actions with other western navies; more than half (163) took place after the UN Charter went into effect in 1945. Robert Mandel, *Effectiveness of Gunboat Diplomacy*, INT'L. STUD. QTRLY, offers a survey of 133 incidents between 1946 and 1986, finding a high proportion secured the desired response from the target state.

"imperfect war," to characterize aspects of the "war on terror" – something that is more than law enforcement but less than full-blown "war."[82]

Many commentators, it is true, hold that the UN Charter has superseded all such practices.[83] 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." It might be that such restrictions don't apply, in any case, to countermeasures in cyber space, 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 …."[84] Resolutions of the UN General Assembly have sought to emphasize that the Charter prohibits the "threat of force" along with the "use of force."[85]

---

[82] Gregory E. Maggs, *Assessing the Legality of Counter-terrorism Measures Without Characterizing Them as Law Enforcement or Military Action*, George Washington University Law School, Public Law and Legal Theory Working Paper No. 257 (Feb. 26, 2006); Kathryn L. Einspanier, *Burlamaqui, the Constitution and the Imperfect War on Terror*, 96 GEO. L. J. 985 (2007)

[83] A leading commentary on the UN Charter puts it this way: "lawful self-defense is restricted to the repulse of an armed attack and must not entail retaliatory or punitive action." Bruno Simma et al., THE CHARTER OF THE UNITED NATIONS: *A Commentary* (2d. ed, 2002) at 792.

[84] Art. 2, Par. 4 (emphasis added)

[85] Notably, "Resolution on the Non-Use of Force in International Relations," GA Res. 2936, Nov. 29 1972: "The General Assembly … Believing the renunciation of the use *or threat of force* … should be

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. 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 U.S. 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.[86]

A quarter century later, President Reagan deployed the Navy to the Gulf of Sidra, challenging the Libyan claim that the open bay constituted Libyan territorial waters and so could be closed to international navigation. The presence of American warships provoked an armed exchange with Libyan patrol boats after which several of the latter were sunk by American warships. But the entire exchange was deemed less risky than an actual land invasion of Libya.[87]

---

fully observed as a law of international life, Solemnly declares, on behalf of the States Members of the [UN] Organization, their renunciation of the use *or threat of force* in all its forms and manifestations in international relations, in accordance with the Charter of the United Nations …." (emphasis added)

[86] GRAHAM ALISON and PHILIP ZELIKOW, ESSENCE OF DECISION: EXPLAINING THE CUBAN MISSILE CRISIS (1999)

[87] JOSEPH T. STANIK, EL DORADO CANYON: REAGN'S UNDECLARED WAR WITH QADDAFI (2003), p. 52

During the Iran-Iraq war in the late 1980s, the United States took "active measures" to protect international oil shipping, deploying the U.S. Navy to the Persian Gulf. While in the area, the Navy mistakenly attacked an Iranian passenger jet – a mistake for which the United States ultimately paid reparations. But the presence of the Navy in the first place was an implicit threat to use force.[88] In many minor episodes, a naval fleet has been deployed to a troubled part of the world to register American concerns, but the deployment of an aircraft carrier is not usually taken as mere token of sympathy.[89]

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 shorts 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.

---

[88] HAROLD LEE WISE, INSIDE THE DANGER ZONE: THE U.S. MILITARY IN THE PERSIAN GULF 1987-88 (2007)

[89] EDWARD N. LUTTWAK, THE POLITICAL USES OF SEA POWER (1974): "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 suasion is therefore … 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." (pp. 12-13)

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?

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

IV. Permissible Targets and the Problem of Attribution

According to the International Committee of the Red Cross, international law already has an established rule that forbids attacks on civilian infrastructure, even

in cyber space.[90] The argument is beguilingly simple. It starts by invoking the most comprehensive convention on the law of Armed Conflict, Additional Protocol I (1977) to the Geneva Conventions (AP I).[91] 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."[92]

AP I defines "military objectives" as all those targets whose "partial or complete destruction" would offer "in the circumstances ruling at the time, a definite military advantage."[93] 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*."[94] 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."[95]

---

[90] International Committee of the Red Cross, *Cyber warfare, 29-10-2010 Overview*, available on ICRC website: www.icrc.org,

[91] Additional Protocol I to the Geneva Convention of 1949, June 8, 1977, 1125 U.N.T.S. 3

[92] Art. 48

[93] Art. 52, Par. 2

[94] Art 52, Par. 1 (emphasis added).

[95] ICRC, "Overview," p. 2. For elaboration of the arguments behind this conclusion, see Knut Doermann, *Computer Network Attack and International Humanitarian Law*, CAM. REV. INT'L. AFF. May 2001 (available on icrc website).

One obvious problem with this conclusion, in relation to American policy, is that the United States is not a party to Additional Protocol 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.[96] Many commentators on cyber conflict take for granted that attacks on "civilian objects" are now forbidden by international law, even in the cyber realm.[97]

The United States government expressly rejected the ICRC study as any reliable guide to customary international law.[98] The ICRC study relies almost entirely on statements of intention by governments, many of which are clearly rhetorical or misleading.[99] 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

---

[96] J-M HENCKAERTS and LOUISE DOSWOLD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW (2005), Vol. I, p. 25 (Rule 7)

[97] Id.

[98] John B. Bellinger (Legal Adviser for the Department of State) and William J. Haynes (General Counsel for the Department of Defense), *A U.S. Government response to the ICRC study Customary International Humanitarian Law*, INT'L. REV. RED CROSS (866), June 30, 2007

[99] 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 (Vol. II, p. 146) or similar statements from Saddam Hussein. It even invokes statements by opposition politicians, criticizing government policy – and then treats the opposition criticism as somehow more authoritative than the government policy it criticized. (II, 310) 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. (II, 236 – Human Rights Watch; II, 331 – ICRC; II, 369 – Amnesty International).

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 Sec. 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 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. 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, because 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."[100]

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 week, 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."

---

[100] See notes __ [15] and ___ [21] supra. See also the 1907 Convention XI, "Relative to Certain Restrictions with Regard to the Exercise of the Right of Capture in Naval War," (205 CTS 367-80) which imposed certain humanitarian restrictions on the treatment of captured crews, but did not otherwise restrict the existing practice of seizing enemy merchant ships and their cargoes as prize of war.

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" 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. Commentators argued that even blockade was more "humane" than full-scale invasion. 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 has the capacity to offer this kind of more "humane" war.

In a more intense conflict, the cyber weapon might actually trigger unsought escalation if targeted on 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, provoke 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.[101]

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 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 of 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

[101] JENNIFER E. SIMS, ICARUS RESTRAINED: *An Intellectual History of Nuclear Arms Control* (1990)

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 the "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.[102] 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 local operator, transferring data between his office network and his personal laptop, after the latter had been

---

[102] Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U.J. INT'L. L. 57 at 98-109; Finding #7, NATIONAL RESEARCH COUNCIL (William A. Owens, Kenneth W. Dam, Herbert S. Lin, eds.) TECHNOLOGY, POLICY, ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES (2009), pp. 1-18; Graham Todd, *Armed Attack in Cyberspace*, 64 A.F. L. REV. 65 (2009) at 93-98; Duncan B. Hollis, *An e-SOS for Cyberspace* 52 HARV. INT'L. L. J. 373 (2011) at 397-403; Erik Mudrinich, *Department of Defense Strategy for Cyberspace and the Attribution Problem,* 68 A.F. L. REV. 167 (2012) at 190-205.

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 a dozen people 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 (the Italian Red Brigades, the German Red Army Fraktion, etc) 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 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.[103]

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.

---

[103] "Today'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 cyber attack 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." *Id.* At 41.

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 resorted 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. 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 U.S. 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.

V. Who are lawful combatants in cyber space?

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.[104]

And 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 deploy privateers to attack Union commerce on the high seas. The United States government held that, if captured, Confederate privateers should be treated as pirates, not as prisoners of war.[105]

The first thing to notice, however, is that 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. By the 1860s, Confederate privateers were alone in the world.[106] The opposite is true in cyber space.

Even in land warfare, the trend in the Twentieth Century was to be more accepting of auxiliary units, militia, volunteers, if they engaged in organized military operations though not part of the regular military.[107] AP I actually grants prisoner of

---

[104] With specific reference to cyber operations, see Sean Watts, *Combatant Status and Computer Network Attack*, 50 VA. J. INT'L. L. 391 (Winter 2010); SUSAN BRENNER, CYBERTHREATS: THE EMERGING FAULTLINE OF THE NATION STATE (2009), pp. 196-199. Both reason from eligibility for PoW status under the 1949 Geneva Convention (III) on Prisoners of War – disregarding subsequent changes introduced by the 1977 Additional Protocol I.

[105] STEPHEN C. NEFF, JUSTICE IN BLUE AND GRAY, A LEGAL HISTORY OF THE CIVIL WAR (2010), pp. 22-24 (on Union prosecutions of Confederate privateers).

[106] Nicholas Parrillo, *The De-Privatization of American Warfare: How the U.S. Government Used, Regulated and Ultimately Abandoned Privateering in the Nineteenth Century*, 19 YALE J. L. & HUM. 1 (2007)

[107] Hague Convention IV, Respecting the Law and Custom of War on Land (1907), Oct. 18, 1907, 205 C.T.S. 227 (36 Stat. 2277). Annex I, Art. I: "The laws, rights and duties of war extend not only to

war protection to guerilla fighters, even if they have no accountability to a government and conceal their status as fighters until the moment of their attack.[108]

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 attacker. 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 U.S. government allocates some cyber operations to the National Security Agency – as the efforts to undermine the Iranian nuclear program indicate. The restriction in the 2012 Defense Authorization Act, requiring offensive operations in cyber space to conform to the "laws of armed conflict," applies by its terms only to operations conducted by the Department of Defense. There are no counterparts to that restriction in appropriations (or other legislation) affecting NSA or other government agencies. Some targeting of drone strikes against terrorists has already been entrusted to operatives of U.S. intelligence agencies,

---

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."

[108] AP I, Art. 44, Par. 3: "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" [i.e., not always]. Par. 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."

rather than uniformed personnel in the military services.[109] 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 Sec. II, 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. Some commentators have urged that the practice be encouraged and expanded.

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

[109] Despite criticism from critics like Mary Ellen O'Connell: *Unlawful Killing with Combat Drones*, Notre Dame Legal Studies Paper No. 09-43 (2009)

already become targets. General Keith Alexander, Director of the National Security Agency (and Commander of Cybercommand) 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]."[110] Others have estimated other losses to American business from cybercrime (other than from direct theft of IP) as well over $300 billion per year.[111]

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. Then there is a vast amount of more direct theft, using so-called spider programs to transfer information – including patent or trade protected secrets – from owners to commercial rivals, most often in foreign countries (where their operations are not readily subject to legal recourse through U.S. courts).[112]

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, with specialists on laundering money and so on. There are now private online forums serving a cyber black market, where specialists offer

---

[110] Speech at American Enterprise Institute, July 9, 2012. For a summary, see : http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion

[111] Senator Joseph Lieberman (I-Ct), co-sponsor of one of the main proposed bills on cyber security in 2012, endorsed an estimate of $338 billion (annually) to cybercrime (other than direct theft of IP): http://www.lieberman.senate.gov/index/cfm/news-events/news/2012/7/lieberman-pushes-for-cybersecurity-bill-as-government-announces-costs-of-cyber-theft. That estimate appeared in his bill (S. 21, 2012 at p. 2).

[112] FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS IN CYBERSPACE, Report to Congress by the Office of the National Counterintelligence Executive, October 2011. Available online: http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

such services to would-be criminals.[113] A criminal can purchase access to large numbers of hacked machines around the world – with prices varying from $8 to $180 per thousand hacked machines.[114] 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 (and/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.[115] 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

---

[113] J. Franklin, V. Paxson, A. Perrig, and S. Savage, *An inquiry into the nature and causes of the wealth of internet miscreants*, PROC. ACM CONF. ON COMP. & COMMUN. SEC'TY. *(CCS)*, 2007.

[114] J. Caballero, C. Grier, C. Kreibich, and V. Paxson. *Measuring Pay-per-Install: The Commoditization of Malware Distribution*, PROC. USENIX SEC'TY SYMP. , 2011. (Given Outstanding paper award)

[115] Grover Clark, *The English Practice with Regard to Reprisals by Private Persons*, 27 AM. J. INT'L. L 694 (1933)

piracy on the seas (except in a few specially 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 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 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.[116]

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

[116] "… 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 …." Howard Levie, *Submarine Warfare*, at 41 – though Levie goes on to note that the designation "defensive" might be challenged since "they usually opened fire immediately upon sighting a U-boat …."

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.[117] Private companies are allowed to hire armed security guards (and there are more security officers in private pay today than on public payrolls[118]). It is anomalous to insist that no right of self-defense should be available to 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 gangs and government-sponsored predators is often quite smudged in the cyber realm – as it often was when pirate ships stalked the open seas.[119]

Network infrastructure (and computer systems in general) are usually privately owned. Companies like Verizon and ATT, not the government, operate the Internet backbone. Unlike past land conflict, the domain of the conflict in a cyber-war necessarily involves civilians. As a consequence, any computer security

---

[117] District of Columbia v. Heller, 554 U.S. 570 (2008); McDonald v. Chicago, 561 U.S. 3025 (2010)

[118] It was estimated at the beginning of the present decade that some 2 million security officers and guards were in private service, compared with 700,000 public policy officers: Amy Goldstein, *More security firms getting police powers*, SAN FRANCISCO CHRONICLE, Aug. 23, 2010

[119] See notes __ [17] and ___ [50], supra.

strategy is ultimately going 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, co-operation.

And cooperation is important because private companies and research institutions have far broader and deeper technical capabilities than the government alone can muster. Cyber-command and the National Security Agency 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. The annual revenue of Microsoft was more than ten times that. [120]

Private firms can offer much larger salaries to researchers and more desirable working conditions (including the opportunity to exchange research findings with colleagues elsewhere – something that government bureaucracies often find it necessary to restrict, particularly in national security 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 Cold War, the United States encouraged

---

[120] http://www.google.com/finance?q=NASDAQ:SYMC&fstype=ii
and http://epic.org/privacy/surveillance/spotlight/0106/

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 – which acknowledged that, as a matter of international law, support for foreign rebels was not itself an act of unlawful aggression if the insurgents were not under direct command of the sponsor.

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 governments most hostile to the United States rule by authoritarian means and try to suppress open, peaceful dissent in their own territory. Almost all of them try to prevent their own people from having access to free communication. 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.[121] It might do more and more widely. *The New York Times* caused a stir in China when it revealed that relatives of the current premier had accumulated vast

[121] Technological assistance cannot 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. https://www.torproject.org/about/overview.html.en .

wealth.[122] 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 cyber space – may be a very useful way of putting pressure on such governments.[123] The fact that the people at the tip of such measures are civilian is in no way an 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 which aids groups that it does not directly control.[124] 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.

---

[122] David Barboza, *Billions in Hidden Riches for Family of Chinese Leader,* THE NEW YORK TIMES, Oct. 25, 2012. The Chinese government quickly blocked Internet access to this story and to a Chinese translation: http://www.cbc.ca/news/world/story/2012/10/28/china-wen-family-wealth.html

[123] Patrick W. Franzese, "Sovereignty in Cyberspace," 64 A.F. L. REV. 1 (2009) at 34-37, offers argument for more assistance in this area.

[124] Nicaragua v. United States, 1986 ICJ at 146-47.

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.

VI. 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, such as DNS, the global name lookup system, BGP, the Internet's routing protocol, or the cryptographic certificates that underpin security protocols like SSL. Disruptions to these services could paralyze network services worldwide.[125]

It will thus be extremely important – and strategically valuable – to isolate,

[125] In 2008, a botched effort at censoring YouTube in Pakistan resulted in global disruptions. See http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study for details.

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.[126] 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 cyber space, 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 cyber space.

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 which have pledged to cooperate in tracking cyber threats – and expressed their commitment to do so by ratifying the convention – from states which 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

[126] Text at: http://conventions.coe.int/Treaty/EN/Treaties /html/185.htm (2001)

government routinely denies any involvement in such attacks – but has never acknowledged responsibility to assist in identifying and punishing those who were involved. American protests, if any, have not been made public.[127] 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 U.S. countermeasures in cyber space. 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. 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.

If we think seriously about organizing the capacity to retaliate in cyber space, 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.

---

[127] Graham H. Todd, "Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition," 64 A.F.L.REV 65 (2009) at 87-88

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 countries.[128] That approach 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.[129] 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

---

[128] Microsoft Corp. et al. v. John Does 1-39 (U.S. Dist. Ct., E-NY): http//www.zeuslegalnotice.com/images/Complaint_w_Appendices.pdf
For a brief account of the background, "Malware inserted on PC production lines," BBC NEWS – TECHNOLOGY, Sept. 13, 2012 (http://www.bbc.co.uk/news/technology-19585433)

[129] Jay P. Kesan and Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*," 25 HARV. J.L. & TECH. (2012) reviews current legal hurdles, esp. at pp. 474-87

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.[130] 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, since the owners never gave permission for this sort of vigilante action. 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 countermeasures by letting them claim ownership of website addresses or other assets seized from cybercriminals.[131]

---

[130] "Your botnet is my botnet: analysis of a botnet takeover." PROC. ACM CONF COMP & COMM. SEC'TY (CCS '09) Available online: http://dl.acm.org/citation.cfm?id=1653738

[131] The government has already held successful auctions for website addresses seized in the course of law enforcement operations. For accounts of seizure of domain names used for illegal Internet gambling, see: Frank Michlick, *U.S. Government seizes Poker Domains* DOMAIN NAME NEWS, April 4, 2011; Michael Berkens, *ICE Seizes 70 More Domains,* THE DOMAINS, July 12, 2012.

A second response would be to clarify, in 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 have seen foreign predators stealing sensitive technical secrets by 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 Sec. III, one of the main purposes of authorizing privateers was to impose costs on adversaries short of committing to all-out war. We would forego the tactical advantages of cyber retaliation if we regarded it solely as an adjunct to actual shooting wars with real bullets.

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.[132]

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.

VII. 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

[132] http://www.armytimes.com/news/2012/01/military-afghanistan-condulence-payments-millions-012312w/

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.[133]

Other commentators have argued that with all their potential for catastrophic harm to civilians, cyber attacks would 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 which 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 cyber space by negotiating formal agreements never to deploy cyber attacks for military purposes.[134]

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

---

[133] For example: Daniel B. Silver, *Computer Network Attack as a Use of Force Under Article 2(4) of the UN Charter*, 76 INT. L. STUD. 73 (2002); Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*," 47 HARV. INT'L. L.J. 179 (Winter 2006); Duncan Hollis, *Why States Need an International Law for Information Operations*, 11 L. & C. L. REV. (2007), RICHARD CLARKE and ROBERT KNAKE, CYBERWAR (2010), pp. 238-55; Robert Knacke, Council on Foreign Relations, *Internet Governance in an Age of Cyber Insecurity* (2010), pp. 21-23; Andy Johnson and Kyle Spector, *Deterring Cyber War: A U.S.-Led Cybersecurity Summit* (Third Way, Idea Brief, Oct. 2010); Oona Hathaway, et al., *The Law of Cyber-Attack,* 100 CAL. L. REV. 817 (2012), pp. 880-82.

[134] For one of the most recent versions of this argument, see the paper by Bruce Schneier: http://www.schneier.com/blog/archives/2012/06/cyberwar_treati.html

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.[135] 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 which the United States could not accept.[136] No matter how extreme one's vision of all-out cyber war, it could hardly be as horrifyingly destructive as a war fought with nuclear weapons. Appeals to abolish atomic weapons date 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 Sec. II, the Washington Naval Treaty of 1921 prohibited unannounced submarine attacks on civilian shipping. The prohibition was reaffirmed in the 1936 Protocol. And it was completely disregarded by Germany

---

[135] It is customary, in arguments of this kind, to invoke the ill-fated Kellogg-Briand Pact of 1927, which purported to outlaw war. 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. 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.

[136] A problem emphasized in Christopher Ford, *The Trouble with Cyber Arms Controls*, THE NEW ATLANTIS (Fall 2010) and Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, Hoover Institution ("A Future Challenges Essay," 2011).

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 no means to verify that potential enemies were actually also 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 conducted 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.[137]

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 and harassing 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.

---

[137] During the Falklands War, even the Royal Navy's sinking of an Argentine warship, *General Belgrano,* provoked some controversy because the attack (by submarine) occurred outside the immediate domain of military operations. Relatives of Argentinian victims tried to hold the British government responsible in the European Court of Human Rights, but the suit was dismissed on technical grounds. *Belgrano Legal Action Fails*, BBC NEWS REPORT, July 19, 2000

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 we are prepared to retaliate against and then think more concretely about what retaliatory actions would be appropriate. Current U.S. 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. To insist that cyber retaliation should never be used against "civilian objects" is to draw a line we cannot actually maintain. Cyber attacks already strike civilian objects – routinely and pervasively. The challenge is to signal our readiness to respond, without making threats we cannot fulfill.

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.[138] When we fail to respond to lesser challenges, we risk signaling irresolution in facing

[138] JOSEPH WHEELAN, JEFFERSON'S WAR, AMERICA'S FIRST WAR ON TERROR, 1801-1805 (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. Pp. 3, 40-54.

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 the sea were determined by the major sea powers. And a sufficient number of rights and restraints were settled that they occupied large chunks of standard international law treatises down to the early 20th Century.[139]

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

---

[139] See, e.g., T.J. LAWRENCE, PRINCIPLES OF INTERNATIONAL LAW, 5th ed., 1910, pp. 450-508 ("Enemy Property at Sea"), 655-674 ("Neutral Commerce"); 675-696 ("Blockade"); 697-723 ("Contraband"). Or WHEATON'S ELEMENTS OF INTERNATIONAL LAW, 5th ed. (edited by Coleman Philipson, 1916), pp. 546-628 ("Maritime Warfare"); 663-693 ("Neutrality in Maritime Warfare"); 698-714 ("Neutral Commerce"); 714-752 ("Contraband"); 767-789 ("Blockade"); 789-799 ("Visit and Search"); 799-802 ("Neutral Prizes"). Or W.H. HALL, TREATISE ON INTERNATIONAL LAW, 8th ed. (edited by A. Pearce Higgins, Oxford, 1924): pp. 765-900 (on "contraband," "carriage in neutral vessels," "blockade," "neutral goods in enemy's ships," "visit and capture").

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 brings it home to 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 International Criminal Court, has completed only one prosecution since it began operation in 2002. The states known to be most active in developing cyber attack capabilities – Russia, China, Iran, 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 holding governments accountable for cyber attacks that 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 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.