AN EMERGING THREATS ESSAY

# To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict

by Jeremy A. Rabkin and Ariel Rabkin

Koret-Taube Task Force on National Security and Law
*www.emergingthreatsessays.com*

task force on national security and law

## Introduction

For almost two decades, military analysts have worried that foreign powers might use computer networks to inflict harm on the United States. Politicians quickly translated those concerns into warnings of a "cyber Pearl Harbor."[1] Almost as promptly, legal analysts began dutifully charting the limits on how we would fight the cyber war that might follow such an attack—if we chose to conform to the UN Charter and various post-war Geneva Conventions.[2]

But cyber attacks are already a persistent and disturbing aspect of international relations in the twenty-first century. At moments of particular tension between hostile states, computer network attacks have been launched against national infrastructure, causing large-scale disruptions. It happened in Estonia in 2007, Georgia in 2008, and South Korea in 2011. Meanwhile, large and important American companies, including Google, Lockheed Martin, and RSA, have fallen victim to highly sophisticated, multi-stage attacks. These attacks appear to have been encouraged or aided by national governments seeking economic or strategic advantages.[3] So-called "advanced persistent threats"—from highly skilled attackers with deep knowledge of the target—are a major headache for American companies.

So far, the United States government has responded with earnest but vague calls to strengthen international norms of good behavior in the cyber realm. Hostile forces are already probing our defenses and testing the limits of our patience. The Obama administration's International Strategy for Cyberspace suggests the U.S. could retaliate with "military force"—implying that if there really is a devastating cyber attack, we might respond with conventional bombing.[4] As a general strategy, that has some obvious limitations. Would we actually risk war with China or Russia in response to a

HOOVER INSTITUTION
STANFORD UNIVERSITY

cyber attack? What if we traced the attack to a state that officially denied any role in it? What if American intelligence could not prove that the government of that state had condoned the attack? While it threatens military responses, the administration's strategy document makes no mention of the possibility of responding to cyber attacks from foreign countries with counter attacks in the cyber realm.

Meanwhile, Congress—on its own initiative—enacted legislation that "affirms" that the Department of Defense, "upon direction of the President, may conduct offensive operations in cyberspace to defend our Nation, Allies and interests. . . ." This provision in the 2012 National Defense Authorization Act stipulates that such "offensive operations" are "subject to the policy principles and legal regimes that the Department follows for kinetic capability, including the law of armed conflict."[5] But it does not say whether other agencies of government can also undertake or sponsor cyber attacks—nor whether other agencies would be subject to the same "policy principles and legal regimes."

There are good reasons for hesitation or equivocation. The world has never experienced a sustained conflict between major powers in cyberspace. We don't know how far such a conflict might escalate or how easily it might trigger responses with more destructive weapons. We don't know how third parties might react, or all the ways they might be affected. There are good grounds for assessing our options with caution, for not waving cyber swords at potential adversaries, for not trying to defend cyberspace with blogging-style bluster.

But some part of our current hesitation seems to reflect the influence of legal cautions that are not really appropriate. Stewart Baker, former Assistant Secretary for Policy at the Department of Homeland Security, warns that government lawyers have been "tying themselves in knots of legalese . . . to prevent the Pentagon from launching cyberattacks" so the Defense Department has "adopted a cyberwar strategy that simply omitted any plan for conducting offensive operations."[6] Concerns about disrupting international law seem to be a major inhibiting factor in formulating a serious cyber strategy. Or perhaps, as Columbia University law professor Matthew Waxman has argued, appeals to international law limitations are simply convenient trumps for bureaucratic rivals to play against each other in the endemic turf wars of American security policy.[7]

In exploring the options for dealing with a cyber attack from abroad, we should at least try to shake off the constraints of outdated or irrelevant legal norms. The UN Charter was designed to prevent another world war. Whatever benefits we have obtained from that framework over the past sixty years, the Charter regime has coincided with hundreds of small wars and a number of large wars to which the Security Council remained largely irrelevant. The post-war Geneva Conventions sought to repress the worst atrocities of the Second World War. Whatever their success in that respect, they have not been conscientiously observed even in conventional wars. It is highly unlikely that these arrangements—designed for military warfare in a far different world—will

more effectively contain cyber conflicts today. We would do better to heed the words of our greatest wartime president, Abraham Lincoln: "As our case is new, so we must think anew and act anew."

We do not argue that cyber conflict should be viewed as something so novel that it transcends all previous legal categories. To the contrary, past experience can be instructive in framing strategies and categories for dealing with cyber attacks. Cyber conflict bears some similarities to past methods of warfare and might be usefully regulated under legal categories used in international law in earlier times. But cyber conflict does not resemble the kinds of land-based military incursions that the drafters of the UN Charter and post-war Geneva Conventions were trying to control. When we look for legal categories for controlling cyber conflict, we need to look even farther back, to categories the framers of the U.S. Constitution would have recognized from their experience with warfare in the eighteenth century.

## "Armed Attack" vs. Intolerable Activity

Much has been written on the question of when—or whether—a cyber attack can be considered an "armed attack." The issue concerns many commentators because Article 51 of the UN Charter seems to limit the "inherent right of self-defence" to situations where "an armed attack occurs." Under a strict reading of the Charter, states can only deploy force when responding to an "armed attack" or when they are authorized to act by formal resolution of the UN Security Council. On that view, before we threaten forcible retaliation, we must first determine the kinds of attack for which the Charter authorizes the use of force in self-defense.

On the one hand, individual hackers with no political motivation often launch computer-generated attacks that are equivalent to burglary or vandalism—mischief that is annoying to the victims but not particularly damaging or costly to repair. No one seriously imagines that the U.S. Department of Defense needs to be on call to respond to attacks of that sort. But an attack that disabled the U.S. air traffic control system, causing jet liners to crash and killing thousands of civilians, would be quite a different challenge. It might be regarded as equivalent to the 9/11 attacks and might well be thought to demand a decisive, even a devastating, military response. If we want to think seriously about responding to cyber attacks, we will need to clarify the different kinds of attacks that might justify various kinds of responses.

The UN Charter doesn't help us here. If we decide to retaliate in the cyber realm, the ambiguities of classification will cut both ways. Michael Schmitt, a prominent scholar of the law of armed conflict, has made this point on several occasions: If an attack in cyberspace is not an "armed attack"—of the sort that triggers the right to use force in self-defense, under Article 51—then counter-strikes in cyberspace would not require any special justification, either.[8] In fact, Article 41 of the UN Charter contemplates that the Security Council might order "complete or partial interruption of . . . telegraphic, radio and other means of communication" and characterizes such disruptions as

"measures not involving the use of armed force . . ." The same provision mentions "severance of diplomatic relations" among such "measures." So skillful lawyers might depict cyber attacks as equivalent to force—or to mere diplomatic friction.

Such labeling maneuvers do not address the underlying challenge of deciding what sort of law we want to see in cyberspace. If we want norms for proper conduct, we need sanctions for bad behavior: there must be some means of punishing infractions. The existence of UN machinery does not obviate this need for cyber-specific norms because the Security Council can rarely agree on effective measures to enforce international standards. The Security Council is unlikely to impose sanctions in response to cyber attacks because Russia and China, both quite active in developing means of cyber attack, have veto power on the Council.

Long before the establishment of the United Nations, however, states recognized that in most cases, all-out war would be an excessively risky and costly response to provocations. Traditional international law therefore acknowledged the propriety of lesser responses to enforce international obligations—or legitimate methods of self-defense short of war. We can still apply the logic of these lesser responses to deterring cyber attack, starting with "retorsion" and culminating in "reprisal."

Retorsion means something out of the ordinary but not necessarily unlawful, such as denial of ordinary trade benefits. Reprisal embraces conduct not otherwise lawful but justified as a means of forcing others to stop their unlawful practices. Traditionally, wartime measures—so-called "belligerent reprisals"—were used to punish violations of the law of armed conflict, by retaliation in kind. Professor Yoram Dinstein, one of the foremost commentators on the law of armed conflict, insists that armed reprisals also remain a lawful response to peacetime provocations.[9] The State of Israel deploys peacetime reprisals (claiming the right to do so in self-defense) when it launches air strikes in retaliation for terror attacks. The United States has pursued similar measures on occasion. The Reagan administration bombed Tripoli in 1987 in response to terror attacks on off-duty U.S. soldiers in Germany that were traced to the Gaddafi regime. That bombing was not authorized by the UN Security Council, nor was it aimed at repelling an ongoing "armed attack" on the territory of the United States.

When faced with serious provocations, we don't want to be left with a stark choice between utter passivity and all-out war. We need to think about expanding our range of options. The goal should be to identify flexible and proportional responses, rather than fretting about some fixed legal boundary between "attacks" that permit "self-defense" under the UN Charter and those that allow only diplomatic protests. And we are better off exploring those options in advance, before a cyber attack prompts a crisis.

Within the cyber realm, there is a wide range of potential responses that are proportional to the provocation and can be graduated through successive stages of an ongoing confrontation. For the least egregious cyber attack, we might start with a demonstration

of capacity—for example, penetrating computer networks operated by a foreign government and leaving behind mocking messages, as the Chinese have done with computers at the Pentagon and at offices of major American defense contractors. This would be the cyber equivalent of sending a fleet to show the flag in a troubled region.

At a slightly higher level of intensity, we might conduct cyber attacks that are disruptive, but that inflict little permanent damage. Denial-of-service attacks on web businesses already illustrate the potential for attacks of this kind. During the attack, a targeted firm suffers some losses, but the only permanent damage may be reputational. A more severe, government-sponsored attack might disrupt financial or transportation infrastructure for hours or days, without risking physical injury to human beings. So, for example, people would not die if their credit cards were declined due to computer problems. Still, an attack that caused widespread credit card malfunctioning would send a very pointed message.

How far we go might depend not only on the scale of the provocation but also on how sure we are about who should be blamed for it. Current literature on cyber conflict features extensive discussion of "the attribution problem." Because cyber attacks can easily be routed through a chain of networks on different continents, we may not always be sure whether the ultimate responsibility for the attack lies with a particular hostile state. Alternatively, we might trace an attack to a particular group of malicious hackers, but not be sure whether or to what extent they are covertly sponsored by a hostile government. Or we may have strong reasons to believe that a particular state was involved but not want to risk betraying our intelligence sources by presenting our evidence in public.

As novel as the technological setting may be, the underlying problem is not new. It is, in fact, as old as the United States. Even in colonial times, British and French authorities accused each other of conspiring with Indians to attack rival settlements, but it was often difficult to establish "attribution" for any particular Indian raid. As late as the 1980s, U.S. officials protested Soviet and Cuban involvement with guerrilla insurgencies in Central America, while Moscow and Havana routinely denied involvement.

American strategists long ago learned to turn such ambiguities to their own advantage. In the early nineteenth century, the U.S. government cultivated its own ties with Indian tribes in frontier regions and with pirate raiders in the Caribbean, who enjoyed American support when attacking European powers—or at least benefitted from American authorities' turning a blind eye to those attacks. In the 1980s, the United States gave various forms of background assistance to anti-Marxist guerrillas in Nicaragua. When Nicaragua protested to the International Court of Justice, the court acknowledged the United States did not bear direct responsibility for the use of force by "Contra" rebels, because the United States did not exercise direct control over these irregular forces, even if it plainly sought to assist and encourage them.

Similarly, the United States could register its displeasure through a wide range of measures without committing to direct confrontation. In the case of a less serious cyber attack, this might mean funding research in anti-censorship technology or turning a blind eye to private activists trying to breach Internet censorship in target countries. While such measures may pose the risk of escalation, American policy-makers have substantial experience with these risks—and are often willing to take chances on aggressive security measures. For instance, the United States regularly launches fatal drone strikes on terror suspects in countries with which we are not at war. Is a cyber attack really a bigger provocation than bombing?

## Permissible Military Targets vs. Protected Civilian Sites

A good deal of literature insists that retaliatory cyber attacks must remain within limits set by the Law of Armed Conflict (LOAC). The most recent effort to codify LOAC norms, the 1977 Additional Protocol I (AP I) to the Geneva Conventions, emphasizes that attacks must not be launched on civilians or "civilian objects." Commentaries sponsored by the International Committee of the Red Cross in Geneva have emphasized that there are no permissible exceptions to these restrictions and that they apply to cyber attacks just as they do to other methods of war.[10] Quite a few American legal analysts have endorsed this perspective.

But it is a mistake to try to fit cyber retaliation into this framework. Although the United States acknowledges that many AP I provisions are now part of binding customary law, the U.S. has not actually ratified AP I. And several American allies that did ratify the protocol—including Britain, France, Germany, Canada and Australia—did so with formal reservations, claiming the right to engage in reprisals in kind against enemies who violate restrictions in the treaty. Even if we considered all cyber attacks as legally equivalent to "armed attack," and then assumed that all restrictions on armed conflict apply in the cyber realm, the ICRC claim that retaliatory cyber attacks may never be launched at civilians or "civilian objects" is still not persuasive.

The ICRC view wrongly tries to extend rules designed for one kind of warfare to all types of conflict. It is only in the past century that we have tried to codify rules of war in international conventions, but the law of war goes back many centuries. It has long provided separate rules for land war and sea war. The Hague Peace Conferences of 1899 and 1907 thus proposed a convention on "The Law and Custom of War On Land" and a series of quite different conventions on naval warfare.

This legal distinction reflected the different ways conflicts were conducted on land and sea. In conventional land war, the objective was to seize and hold enemy territory. The dynamic of the struggle would invest particular locations with tactical or strategic importance and the presence of civilians was typically a distracting challenge. If they took up arms to resist, civilians could cause trouble for an invading army. So the custom was to promise civilians immunity if they would refrain from participating in hostilities. Restrictions on targeting civilians and civilian property arose from the

perceived common interest of the invading land army and the local citizens. Civilians earned immunity by maintaining neutrality.

War on the sea was different. The purpose of fighting was not to seize and hold territory but to harass the enemy. One method was to disrupt the enemy's commerce by seizing and sometimes sinking enemy merchant ships. Belligerent states did not worry about civilian residents, but a fellowship of the sea did guide the treatment of ships' crews. Belligerents did not want to provoke neutral states, which might enter the fight if their own ships were attacked or they felt threatened by violations of acceptable conduct for naval warfare. So naval powers adhered to limits on the treatment of surrendered crews, whether on warships or merchant ships.

Classic naval warfare thus distinguished permissible from impermissible targets, but the distinction was not between military and civilian targets. Typically, commerce raiders would board a merchant ship, determine its nationality, and if it belonged to the enemy, would seize the ship and its cargo as a "prize of war." If a warship had to sink an enemy ship, it did so only after trying to help the enemy crew to safety. Until the end of the nineteenth century, naval technology made it feasible and safe for commerce raiders to take such precautions when seizing an enemy vessel.

In the twentieth century, this system broke down because radio communication made it possible for merchant ships under attack to request assistance from allied warships. This made it dangerous for attackers to board the captured ship, search it, and see to the crew's safety before sinking it. At the same time, submarines and aircraft proved to be potent weapons—but they lacked any real capacity to board or search the ships they attacked. As a result, lethal attacks without warning became common during the world wars. Allied navies used their surface fleets to blockade enemy shipping lanes, cutting off almost all neutral vessels, even those carrying food and fuel.

If we still recognize land and naval warfare as distinct categories, we must surely classify cyber conflict with the latter. Indeed, cyber conflict has more in common with early naval warfare than with twentieth century naval practices. In cyber conflict, attackers bear little personal risk, and can impose significant economic harm without threatening the lives of civilians. Like sea raiders of old, they will not typically interact, in any direct way, with the civilian population in the target country. Accordingly, cyber attackers do not face the same incentives as land armies to grant combat immunity to enemy civilians.

In a cyber conflict, we still have good reason, of course, to observe humanitarian constraints when civilian lives are at stake. But cyber attacks can inflict economic hardship without bodily harm. So rules designed to prevent civilians from being killed in crossfire make less sense if they are deployed to prevent civilians from suffering economic hardship or personal inconvenience. Thus we need not extend complete

target immunity to what AP I calls "civilian objects"—equipment, installations, and economic infrastructure not devoted to "military" purposes.

In twentieth century bombing campaigns, strategists viewed industrial facilities for arms production as a sort of intermediate targeting case: more appropriate than other civilian facilities, but less so than purely military infrastructure. Though some analysts have claimed it would still be lawful to strike economic targets relevant to the enemy's war-fighting capacity, that sort of analysis does not map very well onto the realities of a conflict that remains in the cyber realm. Cyber conflict would not depend on specialized infrastructure. The computers and software development tools that might be used would be hard—often impossible—to distinguish from those used for purely commercial purposes or civilian-oriented research. If we tried to attack an enemy's "high tech sector" as a military target, we would inflict proportionally as much harm to civilian objects as did World War II bombing, but with far less excuse, since we now have the capacity to be more discriminating in our targeting.

It does not follow, however, that we should want to concentrate exclusively on military computer networks. If anything, attacks on actual military objects, such as command-and-control links, are likely to be more destabilizing than attacks on civilian targets. During a crisis, a mid-level officer who suddenly loses contact with superiors might become jumpy and prone to an overly aggressive response. High-level commanders, threatened with the loss of contact and control over their entire military, may start to think in apocalyptic terms. That would be a particularly ominous development in states where commanders have access to weapons of mass destruction. It would be more prudent to leave enemy military targets alone, rather than risk goading enemy commanders into panicky, "use it or lose it" decision-making.

## Lawful Participants: Soldiers vs. Civilians

In earlier times, the Law of Armed Conflict sought to distinguish "military" from "civilian" not only in terms of targets but also in terms of lawful participation in combat. In large part, this was because the military combatants could not honor the targeting distinction if civilians did not honor the participation exclusion: if every civilian might be a fighter in disguise, armies would have to regard all civilians as potential enemies. So invading armies treated armed civilians with great suspicion and those found using their weapons for combat could be summarily executed. Older treatises described civilian combatants as "war criminals" or perpetrators of "war treason."

Treaties acknowledged some exceptions, however, even in land warfare. The Hague Conventions on Land Warfare and the 1949 Geneva Convention III extended protections for prisoners of war to members of militias and others outside the regular army if they met certain conditions. Those conditions for irregular combatants included carrying arms openly and maintaining at least some insignia on their clothing, indicating their combatant status. Even then, such fighters were only protected if they operated under

a defined command structure and obeyed the laws of war—in other words, if they accepted the legal constraints applying to full-time soldiers.

There is dispute about whether and how these protections should be applied to guerrilla fighters today. Additional Protocol I allows guerrillas to claim prisoner of war status even if they do not carry arms openly nor display identifying insignia before they enter combat operations. Such concessions to guerrilla warfare—which might easily be interpreted to protect even terrorist networks—were a principal reason the U.S. rejected AP I.

But none of these protections makes much sense in a cyber conflict. Cyber intrusion is almost always conducted by stealth: the U.S. Department of Defense will not send destructive cyber messages by email with a return address identifying itself as the sender. There is so much cyber crime and cyber espionage on today's Internet that no country can claim that it relies on the "civilian" character of incoming messages and regards malicious messaging as "perfidy." Cyber warriors—if we want to think of them as warriors—won't have a physical presence in enemy territory. They are highly unlikely to be captured by enemies, let alone need to invoke Geneva Convention protections for prisoners of war.

Nor are civilian hacktivists likely to operate with the military-style discipline of an identifiable chain of command. While some degree of military training is required for traditional combat units to function effectively, the same is not true for citizen hacktivists. The skills they need are well developed in non-military sectors of the information technology industry. Since there are so many non-military threats to computer networks—from criminal gangs, vandals and others—commercial developers and academics in computer science already focus on network security for civilian use. Understanding computer security necessarily means understanding attacks. Papers describing new attack techniques are routine in academic computer security publications.[11] The academic computer science curriculum increasingly includes techniques relevant to cyber conflict. There are organized—and legal—contests in which college students compete to quickly and effectively break into designated computers.[12] Indeed, there are calls for schools to require students to understand malicious software and even to practice writing their own.[13] We might think of citizens with such skills as the high-tech equivalent of citizen militia fighters.

Certainly, if there is a cyber conflict with a publicly identified adversary, there will be many individuals in the private sector who have the technical skills to participate in retaliation—and who may feel a strong temptation to do so. A formal training and command structure, for the purpose of enforcing basic discipline, may not be necessary. Leaving such volunteers entirely without official guidance, however, would make it hard to limit retaliatory attacks and prevent unwanted escalation.

Here, again, we might do well to think about cyber conflict in more imaginative ways, by drawing on much earlier experience. Since cyber conflict has much in common with traditional naval warfare, we should recall that governments often invoked the aid of capable mariners who were not part of the regular navy. Before the mid-nineteenth century, "privateers" were often commissioned to attack enemy ships. They were offered a percentage of what they could seize from enemy commerce. They were distinguished from mere pirates—with whom they had obvious similarities—by formal authorizations, so-called "letters of marque," issued by the sponsoring state.

Privateering was once a common feature of naval warfare, partly for reasons of economy: it allowed governments to extend their force at sea without the expense of maintaining large fleets. There were also diplomatic or strategic advantages. Commissioning privateer attacks was a means of imposing harm on another state without committing to war. Thus the framers of the U.S. Constitution took care to specify that Congress had the power to "declare war" but also the power to "issue letters of marque," implying that the latter could proceed without the former. In interpreting this clause in an early case, the U.S. Supreme Court cited the treatise of the Swiss jurist Jean-Jacques Burlamaqui, who associated the practice with "imperfect war," in which some hostilities are permitted but the conflict remains more constrained than all-out war.[14] In practice, letters of marque often were issued to those who had learned the craft of capturing prize at sea without any government authorization. Governments issuing authorization brought these raiders under more state control in return for offering them more state protection.

Comparisons between cyber warriors and pirates of old are not fanciful. Cyber crime is a pervasive aspect of today's Internet. Much like international drug dealers, cyber criminals have sought protective relations with sympathetic or accommodating governments. The so-called "Russian Business Network," active in a range of cyber crime activities, seems to have received protection and support from the Russian government.[15] The Chinese government has openly encouraged private hackers and may well have enlisted organized groups to probe Western business and government networks—and then take or sell what they can.[16]

Professional computer criminals are a deep reservoir of technical talent. A government seeking to conduct a cyber conflict on the cheap might tell criminals "we will protect and aid you with our diplomatic and intelligence resources, provided you direct your criminal enterprises against our enemies." Using proxy combatants of this sort may reduce the risk of escalation. Criminals are restrained in ways that ideologically-motivated combatants are not. A criminal's goal will not be to render cities uninhabitable, or to cripple economic infrastructure, but rather to divert profits from ongoing commercial activities.

Just as in past conflicts, the target state is likely to be highly affronted by direct attacks from another government. Attacks by shadowy networks may be harder to retaliate

against. Elsewhere in the world, governments are already preparing and using such hard-to-trace attacks by non-governmental cyber warriors. The United States should consider ways to respond in kind. That means thinking about a range of possible participants, with varying degrees of government sponsorship, control or encouragement.

Through a variety of actions, governments can encourage or discourage citizen volunteers from engaging in a conflict. The spectrum starts with relaxing normal enforcement standards and culminates with providing overt training and aid to the volunteers. In the course of actual conflicts, the line between what we condone and what we don't is likely to remain fuzzy. We may accept some practices—or retaliate only indirectly—while issuing formal protests and open retaliation for others. Legal analysts would be wise not to draw precise legal lines in this swampy terrain for the time being. We need more experience with the range of possibilities before we start marking them with precise legal tags.

## Espionage vs. Theft and Destructive Action in Cyberspace

Much activity in cyberspace might be described as computer-based espionage. That raises distinct legal challenges. Nations have always felt free to impose criminal penalties for spying. But neither classic treatises on the law of armed conflict, nor the various Hague or Geneva Conventions on the law of war, recognize espionage as an affront to international norms. Even the Statute of the International Criminal Court, drafted in 1998, fails to include espionage in its compilation of war crimes and crimes against humanity. Every modern state feels free to field its own intelligence service.

Such indulgent attitudes are easily explained. No one expects these services to refrain from seeking out the secrets of other states, even in peacetime. States can try to catch and prosecute foreign spies, but it seems pointless to threaten reprisals in kind against the state whose spies have been caught because all states must assume their friends and enemies alike engage in spying. Why make a special fuss, then, about cyber spying?

The reason is that cyber spying often targets private entities. Traditional espionage focused on acquiring military and diplomatic secrets from rival states. In earlier times, private firms or private individuals rarely had secrets sought by foreign governments. The Oxford English Dictionary reports no use of the term "industrial espionage" prior to the 1960s.

Today, cyber attacks are routinely directed against information in private hands. Many companies, particularly technology companies, rely on trade secrets to maintain their competitive advantage. Foreign competitors sometimes attempt to catch up by stealing these secrets. Intelligence agencies in the U.S., Britain, and Germany have all pointed to concerted and sophisticated efforts by Chinese and Russian corporations to gain commercial advantage by intellectual property theft.[17]

Other attacks have sought to disrupt e-commerce—or to demonstrate the capacity to do so—by targeting databases with sensitive information about clients, such as credit card numbers. Criminal gangs share such information with perpetrators of credit card fraud or those who seek to extort protection payments from threatened corporations. While many such attacks simply aim to extract a quick profit, others seek to inflict harm on the target for ideological reasons.

Such ideologically-motivated and publicly-disclosed attacks have become increasingly common. In December 2011, malicious hackers published several thousand Israeli credit card numbers in a politically-motivated attack traced to Saudi perpetrators protesting Israel's alleged abuse of Palestinians. In the United States, the political-consulting company Stratfor was the victim of a similar attack, which seems to have had no larger purpose than to embarrass the conservative-leaning firm and its clients. In January 2012, the hacktivist group Anonymous claimed credit for a mocking revision of the mission statement on the website of the Susan G. Komen foundation to protest that organization's suspension of contracts with Planned Parenthood. Similar attacks have involved publication of internal corporate email to embarrass the target firm.[18]

Some of these attacks may be regarded as little more than high-tech vandalism, the cyber equivalent of spray-painting profanity on a storefront or a factory gate. Improved security practices or improved policing may deter some attackers. But the threat is more challenging when perpetrators are in foreign countries and protected and encouraged by foreign governments. Both Russia and China are known to have organized economic espionage campaigns, supported by national intelligence agencies.[19]

At some point, stealing information from private firms looks less like traditional espionage and more like high-tech looting. The United States government may have its own forms of intelligence gathering, seeking to uncover secrets of foreign governments. It may not want to make much fuss about other governments engaged in parallel activities, because it may reasonably prefer to keep its own intelligence gathering in the shadows. But the government has an obligation to protect its own citizens against looting, against attempted blackmail and extortion, and against abusive revelation of personal information ordinarily kept private. The United States government has a particular responsibility to protect American firms and private citizens from attacks launched by organizations operating from foreign countries and outside the reach of American law.

In earlier times, the United States regarded attacks on Americans and even American property as warranting military intervention. President Woodrow Wilson sent a small army into northern Mexico in 1916 to hunt down Mexican bandits who had committed arson in an American border town, killing or wounding a dozen American civilians. In the early nineteenth century, General Andrew Jackson pursued hostile Indians into Spanish Florida in retaliation for their raids on frontier settlements in Georgia.

Less direct responses were also available. As noted earlier, issuing letters of marque to privateers allowed the government to respond without deploying public force. Letters of marque and letters of reprisal (also authorized in the Constitution) were originally conceived as authorizations to private parties to indemnify themselves for injuries by seizing (or destroying) property from the home state of the original attacker.

Today, we have good reason to be wary about resorting to armed force against foreign states, but we may well choose to retaliate electronically against states that sponsor or condone cyber attacks on American computer networks. Authoritarian states have many secrets that could serve as targets for retaliation. Groups that want to publicize information about the wealth or high-living of government officials in such countries may violate American law if they do so from sites in the United States. We might change our laws to accommodate such groups and allow our government to promise immunity for such actions in appropriate circumstances. At the same time, as cyber policy evolves in the United States, it should acknowledge that active retaliation—using cyber weapons, not military ones—may sometimes be appropriate as a way to deter foreign governments from supporting attacks on our own citizens and our own economic infrastructure.

## Conclusion

As cyber attackers grow bolder in menacing a wide variety of targets around the world, our law must evolve to meet these new threats. While we can draw on some of the categories in existing legal norms, cyber attacks are a new phenomenon in the history of conflict that requires new norms as well. Prior to the twentieth century, international law had to cope with many gray areas in a world that was not so neatly ordered as that envisioned by the UN Charter and post-war Geneva Conventions. In the cyber realm, the lines of conflict have again become blurred. We can begin to meet future cyber challenges by adapting old practices and institutions.

We will have to sort out a great many questions about matching cyber strategy with our internal institutional controls. Which actions should require presidential direction and which should require authorization from Congress? Which measures should be publicly avowed and which should be left in the shadows? What should be regarded as a military tactic under Pentagon control and what is better trusted to non-military actors? Before we become embroiled in these procedural debates, however, we must first try to clarify the range of possible responses available to us in the cyber realm. We must first decide what kinds of cyber attacks require an American response and what kinds of retaliation we are prepared to deliver.

## Notes

1 Defense Secretary Leon Panetta used the phrase at a hearing of the Senate Armed Services Committee on June 9, 2011. 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. A Google search of "cyber Pearl Harbor" now generates nearly 3 million results.

2 See, e.g., Scott Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *Berkeley Journal of International Law*, Vol. 27 (2008), p. 191, esp. pp. 239–45; Thomas C. Wingfield, *The Law of Information Conflict*, *National Security Law in Cyber Space* (Falls Church, Va.: Aegis Research, 2000), esp. pp. 44–46; Duncan Hollis, "Why States Need an International Law for Information Operations," *Lewis and Clark Law Review*, Vol. 11 (2007), p. 1023.

3 Mathew J. Schwartz, "Lockheed Martin Suffers Massive Cyberattack," *Information Week*, May 31, 2011.

4 "International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World," May 2011, p. 14. Available from White House website: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

5 2012 National Defense Authorization Act, Sec. 954. The accompanying conference report (H. Rept. 112–329, Cong. Rec., Dec. 12, 2011) explains that the provision originally appeared in the House bill without the restrictive proviso. The Senate bill had no parallel provision but Senate conferees accepted the authorization, only after House conferees agree to the cautionary addition.

6 Stewart Baker, "Denial of Service: Lawyers are crippling America's ability to defend against cyberwar with arcane rules and regulations," *Foreign Policy*, Sept. 30, 2011.

7 Matthew Waxman, "Cyber-Attacks and the Use of Force," 36 *Yale J. Int'l L.* 421 (2011).

8 The argument seems to have first been developed by Michael Schmitt in "Computer Network Attack and International Law," *Naval War College International Law Studies* (2002).

9 Yoram Dinstein, *War, Aggression and Self-Defense* (New York: Cambridge University Press, 4th ed., 2005), pp. 221–31.

10 International Committee of the Red Cross, "Cyber warfare, 29-10-2010 Overview," available at http://www.icrc.org. For elaboration of the arguments behind this conclusion, see Knut Doermann, "Computer Network Attack and International Humanitarian Law," *Cambridge Review of International Affairs*, May 2001, available at http://www.icrc.org.

11 "Attacks against networks and machines" is the fourth category of papers listed in the Call for Papers at the recent USENIX Security conference, among the top venues for computer security research. (http://www.usenix.org/events/sec11/cfp/topics.html)

12 "The UCSB iCTF," accessed September 20, 2011, http://ictf.cs.ucsb.edu.

13 George Ledlin, "The Growing Harm of Not Teaching Malware," *Communications of the ACM*, February 2011, pp. 32–34.

14 *Bas v. Tingy*, 4 Dall. 37 (1800).

15 Peter Warren, "Hunt for Russia's web criminals," *The Guardian*, Nov. 14, 2007, available at http://www.guardian.co.uk/technology/2007/nov/15/news.crime; Brian Krebs, "Shadowy Russian Firm Seen as Conduit for Cybercrime," *The Washington Post*, Oct. 13, 2007, available at http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html.

16 Ryan Paul, "Researchers identify command servers behind Google Attack," *ars technica*, available at http://arstechnica.com/security/news/2010/01/researchers-identify-command-servers-behind-google-attack.ars.

17 Kate Connolly, "Germany accuses China of industrial espionage," *The Guardian*, July 22, 2009, available at http://www.guardian.co.uk/world/2009/jul/22/germany-china-industrial-espionage.

18 Such attacks have targeted law firms (see http://www.theatlanticwire.com/technology/2012/02/100000-emails-leaked-haditha-marines-lawyers-now-what/48292/), banks (see http://www.theregister.co.uk/2011/03/14/anon_bofa_wikileak/) and other businesses (see http://www.theregister.co.uk/2011/03/01/hbgary_ceo_resigns_over_anon_hack).

19 "Foreign Spies Stealing US Economic Secrets in Cyberspace," US Office of the National Counterintelligence Executive, October 2011.



The preferred citation for this publication is
Jeremy A. Rabkin and Ariel Rabkin, "Why the Current Law of Armed Conflict Should Not Fetter U.S. Cyber Strategy (2012)," in *Emerging Threats in National Security and Law*, edited by Peter Berkowitz, http://www.emergingthreatsessays.com.

***Jeremy A. Rabkin***

*Jeremy A. Rabkin is currently a professor of law at George Mason University (GMU), where he teaches courses including International Law and The Law of War. He holds a PhD in political science from Harvard University. Before coming to GMU in 2007, he taught for many years in the Department of Government at Cornell University. His most recent book is* Law without Nations? *(Princeton University Press).*

***Ariel Rabkin***

*Ariel Rabkin received his PhD in computer science from UC Berkeley in 2012, where he was advised by Randy Katz. His dissertation concerns making software systems easier to configure and manage; he is also interested in security and cloud computing. Rabkin obtained his bachelor's degree in 2006 and his master's in engineering in 2007, both from Cornell University.*

## Koret-Taube Task Force on National Security and Law

The National Security and Law Task Force examines the rule of law, the laws of war, and American constitutional law with a view to making proposals that strike an optimal balance between individual freedom and the vigorous defense of the nation against terrorists both abroad and at home. The task force's focus is the rule of law and its role in Western civilization, as well as the roles of international law and organizations, the laws of war, and U.S. criminal law. Those goals will be accomplished by systematically studying the constellation of issues—social, economic, and political—on which striking a balance depends.

The core membership of this task force includes Kenneth Anderson, Peter Berkowitz (chair), Philip Bobbitt, Jack Goldsmith, Stephen D. Krasner, Jessica Stern, Matthew Waxman, Ruth Wedgwood, Benjamin Wittes, and Amy B. Zegart.

*For more information about this Hoover Institution Task Force please visit us online at www.hoover.org/taskforces/national-security.*

HOOVER INSTITUTION
STANFORD UNIVERSITY