A HOOVER INSTITUTION ESSAY

Hacking Back Without Cracking Up

JEREMY RABKIN AND ARIEL RABKIN

Aegis Paper Series No. 1606

For at least two decades, American firms and institutions have been victimized by attacks on their computer systems. Hackers disrupt their websites, interfere with their communications, and—most costly of all—steal their data. General Keith Alexander, then director of the National Security Agency (NSA), characterized the scale of intellectual property theft by cyber attacks as "the largest transfer of wealth in world history."[1] Estimates place losses to American business at over one hundred billion dollars per year.[2]

In response, American businesses have invested heavily in technology to secure their computer networks from intruders. The most clever and determined hackers manage to work around almost all defense measures, however. Such determined attackers, who spend a great deal of time burrowing deeply into adversary computer networks, are known in the security community as "advanced persistent threats." A sizable portion of the most skillful and relentless computer criminals operate from foreign countries, beyond the reach of American law enforcement. Last year, the director of National Intelligence, James Clapper, acknowledged to Congress that cyber attacks on American business were increasing and will likely continue to increase.[3]

For the past decade, at least, frustrated computer security specialists have muttered about the appeal of retaliatory measures—so-called hack-back operations. There has been much talk about the appeal of such tactics and the possible risks involved. So far, all these exchanges have simply generated more talking points—at least in public. The debate has been pursued at a high level of abstraction. Even advocates tend to restrict themselves to generalities about the need for "active defense" measures without spelling out concrete proposals.

After years of debate about the need to address computer security, Congress enacted the Cybersecurity Information Sharing Act (CISA) in December of 2015.[4] CISA encourages sharing of information, in various ways, about cyber security threats. It vaguely refers to "defensive measures" but neither authorizes nor prohibits actual hack-back tactics.[5] In brief, more talk, no more action.

The Obama administration seems intellectually exhausted by its effort to assure everyone it is taking the problem seriously—without offending anyone. The debate now seems stalled for lack of concrete proposals. This paper aims, in the first place, to put a concrete proposal on the table. It is not a panacea; it is a plausible way forward. We will start by explaining our proposal in detail and the problems we believe it would solve. We then discuss the proposal's strategic rationale at a higher level, how it compares to various past and current practices, and why concerns about the dangers are considerably exaggerated. We conclude by considering the specific legal changes the proposal would require.

A Reasonable Program and the Reasons for It

Suppose an American company is the victim of a computer intrusion. After the intrusion is detected, the company will doubtless reconfigure its systems to remove the attacker's access. The access logs on the victim's system will often point out the network address from which the attack came. But beyond passing it along to law enforcement, there is nothing more the victim can do with this information.

Our proposal gives victims of cyber attacks access to more effective remedies. Department stores hire private investigators to catch shoplifters rather than relying only on the police. So too private companies should be able to hire their own security services. There should be a list of approved hack-back vendors from which victims are free to choose. These vendors would primarily be in the business of identifying attackers and imposing deterrent costs on attackers by providing the threat of retaliation.

Cyber intrusions are often disguised in various ways, as attackers route their activity through computers on a network. Often the immediate source of an attack—or what appears to be the immediate source—may be in a different country or even on a different continent than the actual source. Tracing these pathways is a job for qualified specialists. Sometimes, the path will go through the computers of third-party bystanders, who are disinclined to cooperate with an investigation. Private investigators should have the right to access these machines.

This is, to be sure, crossing a line—what is often regarded as the line between mere "passive defense" (acting within one's own system) and "active measures" that affect the data or computer networks owned by others. There is certainly potential for abuse. We therefore propose that such intrusions, even when aimed solely at securing

information, should be left to specialists who can be trusted not to interfere with innocent third parties beyond what is required for the investigation.

In some cases, it might be enough for the investigation to end with a lawsuit or a referral to law enforcement for prosecution. This applies both to perpetrators within the United States and in friendly developed countries such as Canada, Australia, or European states, where there are reasonable prospects of local prosecution. Law enforcement authorities in such countries lack the resources to investigate most computer intrusions but may be quite capable of prosecuting these crimes once private parties have identified the perpetrators.

Many cyber attackers operate from countries, such as Russia and China, that are disinclined to cooperate with American law enforcement. For these attackers, a mere notice to local authorities is unlikely to have much effect. In such cases, it might be more effective to follow up an initial warning by gathering more information about the perpetrators and then sending a sterner warning: "We have learned a lot about you by probing your email and your computerized records, your finances, personal whereabouts, typical tactics and past victims. We are posting some of this information on public websites in retaliation for your attacks on American corporations."

The US government already employs a somewhat similar form of "name and shame." In May 2014, the US government indicted five named Chinese government employees for hacking into US private companies.[6] In March 2016, the United States indicted several Iranian government employees for cyber attacks aimed at US banks and at controls on a dam.[7] Though there was little chance of making an arrest in these cases, US authorities expressed hope that the associated publicity might have some deterrent effect.[8] In the case of China, there is some evidence of at least a temporary shift in behavior.[9]

The government can do more to follow up. It can impose more direct costs on perpetrators by denying them travel permits to the United States or access to the US banking system. If the hackers are tied to foreign companies that compete with US companies or benefit from the theft of US intellectual property, the US government can threaten (or impose) commercial sanctions of various kinds on such foreign firms.

The financial transactions and intermediaries of cyber criminals may be particularly vulnerable. To be profitable, cyber crime usually requires payments or follow-up

transactions. It requires somebody to pay the criminals for the stolen data; this requires a payment processor willing to facilitate the transfer of funds. These parties—the ultimate buyers and sponsors as well as the financial intermediaries facilitating the transactions—cannot remain fully anonymous. These parties therefore have vulnerabilities even where criminals themselves do not.[10] Cyber crime will become less profitable if the cyber criminals are unable to find banks willing to move their money.

It might even be reasonable to threaten cyber attacks on foreign banking networks that knowingly process the funds of foreign hackers or hacking enterprises. The most direct or coercive measures should be carried out by US authorities or attempted by private security services only with direct government authorization in a particular case.

Still, attempts to impose retaliation and deterrence must start with gathering information about the perpetrators. Private security firms are well situated to gather and supply this information. There has already been information sharing between private firms tracing the source of attacks on their networks and officials in the NSA. In a publically reported episode a few years ago, Google tried to stop cyber attacks originating in China.[11] Private security firms acknowledge ongoing consultations with government even while remaining vague (in public statements) about exactly what information they share and how it is obtained.[12]

Private organizations have demonstrated the capacity for the relevant sort of investigation. Consider the example of GhostNet. In 2009, a group of private researchers, organized as the Information Warfare Monitor and largely based in Canada, released a report describing the design and behavior of a sophisticated espionage program they dubbed GhostNet. The researchers were able to show that GhostNet was installed on a large number of computers that were of strategic interest to China, including computers belonging to foreign embassies and the Dalai Lama. They showed that GhostNet was surreptitiously sending back files, logging keystrokes, and recording audio near the infected computers. The command-and-control servers for GhostNet were based in China. Moreover, Chinese officials were in possession of content (such as e-mails and chat conversations of dissidents) that would have been acquired most easily through cyber espionage. None of this evidence constitutes absolute proof of Chinese government involvement, but the body of evidence as a whole is extremely persuasive. A small number of private researchers conducted the analysis on GhostNet without conducting any sort of counterhacking. Researchers could do even more if they were given broader legal authority.

If more intrusive cyber sleuthing by private security firms is authorized, who would direct their efforts? We envision a system in which private clients would pay licensed security firms. These firms would act only for clients willing to assume the risks involved. Particular industries, such as defense contractors, may elect to hire firms to act on behalf of a client consortium. The financing would remain private, the risks involved would be borne by private firms, and the decision to embrace such ventures left to each firm.

There are three main reasons for a scheme of this kind. First, despite increasingly large corporate investments in cyber defense, American firms are subject to ever larger and more sophisticated schemes for data theft. This is because "passive defense" only screens out the most unsophisticated attacks—those that have already been tried. The rewards for intrusion are more than enough, however, to secure investment in new methods of attack. Nonspecialists may think of cyber security as the counterpart of better locks to stop break-ins. It is more a system of passport controls—in a world where criminals find it easy to counterfeit approved passports and entry inspectors cannot simply stop all entry, at least not for more than brief periods. So as James Clapper, director of National Intelligence, recently told Congress, theft of data in US computer systems has increased continually in the past decade and is expected to continue increasing in frequency and sophistication.[13]

The second reason for a scheme of this kind is that government seems largely incapable or disinclined to deal with the threat. Few local law enforcement agencies have the capacity to respond to cyber crime, and national law enforcement (particularly the FBI and Secret Service) are preoccupied with the very largest crimes.[14] As a senior member of the Los Angeles County Sheriff's Department put it, "Our agency receives a hundred calls a day for cybercrime complaints, and too often the responding officers basically just gave the victim a blank stare or gave them a minimal answer to finish the interaction as quickly as possible."[15] The NSA has tremendous surveillance capabilities. It does not deploy these capacities to protect US data, however, even US government data. That standoffish posture was glaringly illustrated by the wholesale looting of personnel data from the Office of Personnel Management last year as well as similar problems with hacking of communications at the State Department and a variety of other federal agencies and departments in past years.

There may be sound reasons to keep our highest-level spy agencies out of the business of providing ordinary security. Foreign intelligence agencies have always been kept

separate from domestic law enforcement. There are constitutional and historical reasons for this division: we give greater latitude to foreign intelligence gathering than to domestic law enforcement in securing evidence. There are also strategic reasons: we do not want adversaries to know precisely how effective our intelligence agencies are or what techniques they employ.

But even if we wanted to press the NSA into a larger role in protecting private firms, there would be considerable problems setting priorities. The list of victims is long, and the government's resources are limited. Some firms would prefer the risk of continuing foreign intrusions to the risks of publicizing their vulnerabilities or provoking retaliation. Markets are normally used to reconcile divergent priorities: let firms or private institutions decide for themselves whether to hire private security services or deploy armed guards in their buildings. Just as multiple security firms compete for business, with different training, tactics, and expertise, companies needing cyber protection can have various options available.

Third, the private sector will likely develop a greater capacity to handle the threat than government will. Increasing funding to domestic agencies such as the FBI or Department of Homeland Security will accomplish little because cyber protection is not just a matter of putting bodies in uniforms or behind computer screens. The government has been unable to pay as much or hire as quickly as the private sector. The government will not be able to get the best people nor retain them in government service. Attempts to improve government personnel policies in this area will likely prove a generational struggle, not a reform a new president can simply order into effect at one stroke.

Computer science is not rocket science—in part because it does not require nearly the level of capital investment as a space program. Russia and China—and Iran and North Korea—have not landed astronauts on the moon. Still, they have very advanced hacking programs into which they have poured sizable investments. We should think about tapping the strengths of our own private sector when considering how to respond.

A Strategic View

Strategy is the art of exploiting helpful asymmetries and ameliorating disadvantageous ones. In this section, we evaluate our proposal through this lens. We show which asymmetric factors are taken into account and why our proposal is a good fit for the American strategic position vis-à-vis the Internet.

Disruption is more costly to businesses than to criminals. Part of the value possessed by a successful business is that customers can rely on the business being there. Where hacking can force a business to close temporarily, it imposes large costs. Criminals are not required to observe regular work hours, so for them, temporary disruption is unlikely to be a serious concern.

Businesses have valuable assets, and criminal enterprises usually do not. When Sony was hacked in 2014, the estimated costs were in the range of 70 to 100 million dollars.[16] Destructive hacking can often be accomplished by a criminal gang without much infrastructure, many fewer millions of dollars of property in one place. A business facing cyber criminals, then, cannot usefully retaliate in kind against the assets of the criminals. Even if we could destroy the computers and software of the hackers, strikes on such targets would be analogous to using multimillion dollar weapons to target readily replaceable vehicles that happened to be operated by terrorists. These days, the US "war on terror" targets the combatants, not their equipment. Similarly, businesses trying to deter cyber crime should try to impose personal costs and not merely go after the "corporate" infrastructure of cyber predators.

With this strategy, the asymmetries work to the firms' advantage. Businesses may have more property to protect, but attackers have more secrets they need to secure. We live in an open society, but our adversaries do not. Criminals, by nature, require concealment and secrecy. Foreign intelligence operations likewise can be greatly harmed by publicity. Authoritarian regimes rely on pervasive secrecy about how the government operates and how its senior leaders live. In contrast, the activities of the American government and American businesses are already highly public due to our tradition of press freedom and open government. This means that disclosure is in general a bigger threat to cyber criminals than to US firms.

There are some things we would prefer to keep confidential, of course, such as business trade secrets, diplomatic correspondence, and details about American intelligence-gathering programs. All of these kinds of secrets have been divulged in bulk in the last few years, however. To the extent that disclosure is costly to the US government and to American businesses, these are costs that we are already paying. We should try making our adversaries pay them too by allowing American companies to conduct hack-back operations.

Analogies—Distracting and Instructive

Advocates for harnessing private efforts in cyber security have turned to various analogies. After all, they say, we have recruited private assistance for national security measures in the past. In fact, we did so from the earliest days of our republic! Why not letters of marque for the cyber sphere?

We have made that pitch ourselves. It excites many people—and alarms a great many others. For those who like historical analogies, we have also offered a more recent one: arming merchant ships to fight off U-boat attacks in the world wars (as with depth charges). That's also fun—and maybe scary.[17]

But analogies to wartime practices are misleading. Letters of marque authorized the capture of private shipping on the high seas—as a tactic of war. The inducement was the right to retain a share in the resulting loot after providing a cut to the sponsoring government. It was, in effect, licensed piracy—a deal between governments and adventurers, some of whom learned their craft as actual pirates.

Hack-back in the cyber realm, as we envision it, would not be quite analogous—and it would be highly undesirable to let it become so. Security firms should not be securing direct profit from their hack-back activities. If they did (for example, by selling foreign commercial secrets), the practice might pose serious problems, such as the escalation that critics warn about. Conduct of that sort should be cause for removing security firms' authorization or for imposing criminal penalties.

Before burying this metaphor, however, it is worth remembering the reasons governments issued letters of marque in the old days. In England, the practice originated in the thirteenth century when merchants would complain that foreigners had stolen their property, and kings, acknowledging they could provide no redress, would authorize the victims to recapture the stolen goods—or an equivalent from countrymen of the original predators.[18] But those were the days when barons built their own castles and laid siege to each other in the same spirit of self-help.

By the sixteenth century, kings did not tolerate private wars at home—but were still glad to have sea captains attack enemy commerce on the high seas as a tactic of war. It was cheaper than maintaining a large navy. When European states agreed to repudiate privateering in 1856, the United States refused to go along, precisely because it did not have a large navy. At the outset of the Civil War, the United States belatedly tried to

endorse the international ban when the Confederacy resorted to privateering and the Union built a sizable navy to enforce its blockade on southern ports.

If such analogies seem dated—or sensational—we might think of cyber security services as analogous to a great many contemporary practices. At the most mundane level, commercial office buildings, shopping malls, universities, and other large institutions often maintain guards provided by private security firms. These guards are often armed. The US government itself contracts with specialized security services to guard sensitive installations, most often in dangerous foreign settings—as with Blackwater in Iraq. The trend reflects the cost savings involved in hiring private specialists when needed rather than maintaining large forces on the public payroll. Guards employed by private security services often have the benefit of earlier experience in the military or in police work. This is especially true for services that operate in conflict zones, where many are veterans of specialized military forces (such as Navy Seals).

Here the analogy with cyber security firms does work—to a point. These firms, now advising paying clients on ways to prevent or detect incoming attacks, are often directed by individuals who learned about cyber security in prior military service. But the analogy goes too far if it brings to mind back-alley shoot-outs in some tense quarter of a town by the Tigris. Cyber security is not going to generate a hospital ward full of bleeding victims.

If we want to get the risks in proper perspective, we might think about the role of private investigative services at home and private intelligence services in the wider world. In most American states, private investigation agencies are licensed. There are, of course, restrictions on what they can do to obtain information—they may not normally break into a private home, for example, or even engage in wiretapping without the consent of at least one party to a call. They may not engage in blackmail or extortion or sell secrets to those who use these tactics for unlawful purposes.

Within these limits, however, private investigation agencies can gather a great deal of information that the people involved would not want to be known. This is what private investigators are typically hired to do: investigate potential crimes, suspicions of marital infidelity, and so on. Private investigators are often given access to government records not available to the general public. They are not bound by the same range of Fourth Amendment restrictions that limit surveillance by police (authorities may not, for example, keep records on people who come and go without

cause to suspect them of criminal activity, a restriction that does not apply to private investigators or store detectives).[19]

When it comes to international investigations, a good analogy is reporting on human rights abuses. The US Department of State issues reports on abuses in all United Nations member states. Nongovernmental organizations such as Amnesty International and Human Rights Watch produce similar reports on countries where human rights abuses are most serious. The State Department often relies on such private reporting. Some of what is reported is a matter of public record in the countries involved. Sometimes reports include information relayed by victims, their families, or by dissidents who collect accounts of abuses. Compiling or relaying such information is often unlawful in the countries where it occurs. Hardly anyone objects to US reliance on information sources operating in violation of local law to secure information about human rights abuses, even when such information may be quite embarrassing to foreign governments or officials.

The most reassuring and relevant analogy, however, is with current practice in the field of cyber security. There are a number of episodes in which private security firms have traced hack attacks to their sources—that is, gone into computer networks, in the United States and abroad. In 2014, for example, the cyber security firm CrowdStrike published a report on a particular hacking unit "affiliated with the Chinese People's Liberation Army." The report included not only external pictures of the Shanghai office building where the unit operated but also photographs and names of individual hackers involved in its operations.[20] The cyber security firm Mandiant then published a still more detailed report on a different People's Liberation Army hacking unit.[21]

As it happens, NSA itself receives a large share of advice and assistance from private specialists operating under contract with the government. By the early 2010s, 70 percent of the US intelligence budget was spent on contractors, and contractors accounted for a quarter of the intelligence workforce.[22] The practice of authorizing private companies to gather intelligence is hardly new. Our proposal merely extends the scope of what is already a prevalent practice.

It is certainly worth thinking about limits that should be applied to private cyber sleuthing. Where the aim is simply gathering information on hackers already engaged in unlawful intrusions, however, it is silly to react as if this were a proposal to unloose licensed buccaneers to prey on ordinary civilian commerce.

Anticipating Objections: Too Much or Too Little?

The most common objection to hack-back proposals is the danger of hitting the wrong target. That concern might have had more force a decade ago. The technology and practice of tracking has improved considerably in recent years. As the 2016 Worldwide Threat Assessment of the US Intelligence Community puts it, "Information security professionals will continue to make progress in attributing cyber operations and tying events to previously identified infrastructure or tools that might enable rapid attribution in some cases."[23] While attribution is not always possible, it is sufficiently feasible to matter. It was, after all, considered reliable enough for the US government to accuse named individuals of a particular attack in the recent indictment of Iranian government employees for cyber attacks against US banks and an attempted attack on a dam.[24]

There is also this larger point: a hack-back is not the equivalent of drawing a gun on an intruder. Cyber security firms cannot generally expect to strike down intruders in the midst of an attack. Often, intrusions are not discovered until weeks or months after they have occurred. Substantial data heists—by the original hackers—do not typically occur in quick dash-and-grab incursions. Data theft often requires extended probes of a site to determine what sort of data is where. Security firms will typically have time to examine the character of the incursion after the fact. They can then compare it with patterns found in other operations. They might compare notes with other security firms—something now encouraged by the 2015 Cybersecurity Information Sharing Act. They might compare findings with other intelligence sources—not necessarily limited to discoveries by cyber intrusions. Intelligence agencies often obtain valuable information from defectors, from informants, from incautious statements by targeted foreign officials. Hacking is not the only source of information—even about foreign hacking operations.

Still, cyber security firms may sometimes misattribute the source of an attack. Even the most extensive criminal investigations, followed by all the formalities of criminal trial, still sometimes result in wrongful convictions. But security firms would not be imposing a capital sentence for cyber abuses or even lesser criminal penalties. In the first instance, their efforts would generate the moral, political, or economic pressure that comes with being the object of an investigation—something police (as well as private investigators and journalists) routinely impose on their targets. It might go beyond that to something plausibly described as harassment, bullying, or (to be more polite) "targeted sanctions." Still, the risks of misattribution do not seem unacceptably

high. The wrongly accused could present evidence of their innocence, and wrongful identification could be fixed with an apology and a compensation payment. The proposed scheme could be calibrated to give the private investigative firms the proper incentives with regard to the aggressiveness of their hack-backs. A great deal of useful information might be generated in the process.

Many critics of hack-back proposals worry less about misattribution than the risk that a correct attribution will provoke dangerous reactions. If a security firm inadvertently provokes the managers of a Chinese or Iranian hacking program, they may respond with punitive retaliation. The hackers may not limit such reprisals to the specific security firm or even the specific client corporation. They may not care about legal or institutional classifications. They may assume that any attack of any kind can be blamed on the US government and impose retribution on a large segment of American society—by, for example, turning out the lights in a large American city.

Such concerns are not frivolous, but they are not compelling, in themselves. If we worry that probes by private security firms will provoke a massive response, why wouldn't that be true for action by the NSA or any other government agency? The US government sometimes indicts individuals through our criminal process. Why not worry about the provocation there, too? Fear of provocation encourages passivity. If we followed this logic, we would never respond in any way as hostile powers continue to loot American companies of intellectual property and disrupt their operations.

If we acknowledge that some form of response is necessary, responses in the cyber realm are likely to be more readily controlled and calibrated than other sorts of responses. One great advantage of a hack-back is that the response can be very precisely targeted—we can start by sending messages (literally) to particular individuals. Such warnings do not have to be made public. Probably there would be more embarrassment if they were made public, but that might be left to the choice of the target. If there is a furious response from a hostile state, our own government might tell the responsible private security firm to back off—or it might take over direct supervision or control of ensuing escalations.

The United States may say that it is targeting perpetrators of theft of intellectual property owned by private companies—a distinct category of criminal activity—

rather than personalizing disputes about traditional state-to-state espionage. China and other countries may not be impressed by such distinctions.[25] Still, cyber responses remain quite different from blowing up a factory or landing US Marines—responses that are much more difficult to disguise or deny (on either side) and much more difficult to walk away from.

In any event, the risk of setting off a confrontation is pervasive in statecraft. It is certainly not limited to military measures. It can be generated by trade sanctions—or criticism of human rights practices. We sometimes regret stirring up tensions by initial reactions to bad behavior. The reason why we do not disavow trade sanctions (such as antidumping duties) or criticism of human rights abuses is that we assume we can back off if things develop in awkward ways. Consider our shifting responses, in recent years, to human rights abuses in Egypt or Turkey . . . or China. There is no reason to think cyber security is so much more sensitive that we cannot push back at some times and then, if necessary, step back.

Perhaps the better question is whether actions by private security firms can be expected to make much difference. The simplest answer is that we do not know because we have not given these firms much scope to show what they can do. A plausible hope is that publicizing findings—if it comes to that—might isolate the activities of criminal gangs working with shadowy government support: perhaps major governments can be shamed or pressured into keeping their distance from such operators. Perhaps putting some price on such governments' operations will make them choose targets more carefully—going after US government secrets but not private business firms, for example.

Furthermore, gathering information might be no more than an initial step, which might then be followed up with more aggressive sanctions—interfering with bank balances, for example. How and when these should be undertaken is something to consider carefully and probably should be closely supervised by responsible government authorities. But this option will not exist unless there is closer scrutiny of the hackers.

Finally, we should keep in mind that hack-back does not have to be a panacea to be worthwhile. Crime control usually involves multiple tactics that reinforce the desired aim of deterring and dissuading—or diverting—criminals. It might well turn out that the most determined hackers will not be much impressed by the sorts of retaliation

private security firms can impose. Targeted operatives who are rattled might be replaced by operators with steelier nerves. But raising the price to hackers may raise the price to sponsoring governments. There is potential gain in that.

It would be a gain to demonstrate that hackers cannot rifle through American data without leaving fingerprints—and that the US private sector is equipped to check those prints and identify the culprits. This may give governments second thoughts about harboring criminal hackers or giving free rein to their own operatives.

Legalities and Practicalities: How to Start

Do we need a new law? It might helpful, at some point, for Congress to clarify what is permissible when it comes to a hack-back or more modest efforts at tracing the pathways by which attacks occur. The threat of lawsuits by victims would be more compelling if evidence obtained by hacking into an attacker's computers were clearly made admissible in court. But such a statute is not necessary to start experimenting with more active countermeasures.

Some critics of hack-back proposals insist that they are prohibited by the Computer Fraud and Abuse Act or CFAA (18 U.S.C. §1030). That is by no means clear. The statute was enacted in the 1980s, long before current experience with a globally connected Internet. Most of CFAA's provisions prohibit specific offenses—such as accessing computers to acquire government secrets or to obtain "the financial record of a financial institution" to "defraud" or to "cause damage and loss." It is true that the statute also includes a catchall provision covering "whoever . . . intentionally accesses a computer without authorization . . . and thereby obtains . . . information from any protected computer" [(a)(2)(C)].

This prohibition is so sweeping that Professor Orin Kerr of George Washington University Law School has argued it would likely be treated by courts as unconstitutionally vague unless it were given narrower construction.[26] Under the circumstances, defendants could reasonably seek shelter under the rule of lenity—the doctrine that criminal defendants get the benefit of the doubt when courts have to interpret an ambiguous statute. Other legal analysts argue that, in light of common law doctrines favoring self-help by victims of theft (when they do not themselves threaten violent harm), the statute would likely be read by courts to exclude application to hack-backs by hacking victims acting in self-defense.[27]

The telling fact is that the Justice Department has not dared put the question to the test. No one has yet been prosecuted for "access[ing] a computer" for defensive purposes in response to a previous attack, though there have been a number of episodes where such hack-back practices occurred.

Beyond such technical defenses, there is another way around the seemingly all-encompassing language of the CFAA. Among the concluding provisions of the statute is a clarification that it "does not prohibit any lawfully authorized investigative, protective or intelligence activity of a law enforcement agency of the United States, a State or a political subdivision of a State, or of any intelligence agency of the United States" [18 U.S.C. §1030(f)]. It is entirely plausible for federal agencies to read this language as allowing particular cyber security firms to be "lawfully authorized" to engage in "investigative, protective or intelligence activity" on behalf of relevant federal agencies. This argument has already been developed in legal literature.[28]

The Justice Department or the Department of Homeland Security might designate particular private security firms, in tracing the sources of hacking attacks, to share their findings—or publicize them. This approach would retain government control but harness the resources of the private sector and accommodate the security priorities of private corporations prepared to invest in added security. The Justice Department could reassure participating firms that they would not be subject to subsequent liability (at least under CFAA) so long as they did not exceed authorized actions.

We see two good reasons for proceeding in this fashion rather than waiting for a new law before experimenting with more aggressive tactics of "active defense." First, the wait for a new statute may be a very long wait. The Cybersecurity Information Security Act is a very modest measure that encourages sharing of information among private firms. It makes nothing obligatory and ducks almost every hard policy question. It was still years in the making because a lot of rival constituencies have competing agendas in clarifying new restrictions or new permissions—regarding privacy, liability, government surveillance, and so on.

Second, putting new provisions in the US Code is a rather big step, implying a long-term commitment. It may turn out that giving more leeway to private security firms in cyber space introduces a lot of new risks without providing much additional security. We do not think the risks are all that great, and we think it is worth some risk to see

what can be achieved. If we start down this road, however, we should understand that we are undertaking an experiment. We should be prepared to step back if that turns out to be the more prudent course.

A new statute might give discretion to the president or some other official to impose regulations on security firms that include severe restrictions on their activity. But even adopting new regulations can be a contentious and time-consuming affair. And if such a program is started by the next administration, it might be reluctant to call attention to the failure of authorized hack-back tactics and then officially rescinding the whole program. It might also be awkward to engage in official public backtracking if there are loud protests from an unfriendly foreign state—say, China or Iran—and the change in policy then looks like a major concession or an act of appeasement.

For these reasons, we think it would not only be feasible but actually advisable to start experimenting with authorizations of private hack-back measures before enacting revisions of current law. Starting this way would retain adequate official control of new measures without making a public commitment to an entirely new policy posture.

Conclusion

We think the United States should let victims of computer attacks try to defend their data and their networks through counterhacking. The government should maintain a list of companies approved to conduct such operations and allow them to try to find buyers for their services. We suspect that there are a range of viable tactics that such companies could employ. The most promising of these simply involve information gathering. This would sometimes lead to legal action against the criminals. It would sometimes embarrass the patrons and customers of the criminals into cutting ties with them. Sometimes it would result in pressuring the US government into using the tools of public diplomacy. It may turn out that there is no market demand for hack-back, but there is no great risk in letting private security firms try to prove the contrary.

NOTES

1 Keynote address at American Enterprise Institute conference on cyber security, July 9, 2012 (available online at CSPAN archive).

2 See www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html. For even larger estimates, see Paul Hyman, “Cybercrime: It’s Serious, But Exactly How Serious?” *Communications of the*

ACM 56, No. 3 (March 2013), p. 18, available at http://cacm.acm.org/magazines/2013/3/161196-cybercrime-its-serious-but-exactly-how-serious/fulltext.

3 James R. Clapper, Statement for the Record, House Permanent Select Committee on Intelligence, Sept. 10, 2015, www.dni.gov/files/documents/HPSCI%2010%20Sept%20Cyber%20Hearing%20SFR.pdf.

4 S. 754, 114th Congress, included in Consolidated Appropriations Act of 2016 (adopted by the House of Representatives on December 15, 2015).

5 Sec. 102(7)(B) excludes from the definition of "defensive measure" any "measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or data on an information system" of any outside party—but CISA provides no separate prohibitions on such measures. See www.congress.gov/bill/114th-congress/senate-bill/754/text#toc-id9ad6c373f3fd44b3819b45b5a8b19688.

6 See www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

7 Dustin Volz and Jim Finkle, "U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam," Reuters, Mar. 25, 2016, www.reuters.com/article/us-usa-iran-cyber-idUSKCNOWQ1JF.

8 See www.usnews.com/politics/articles/2016-03-25/us-indicts-7-hackers-in-effort-to-send-a-message-to-iran.

9 See www.washingtonpost.com/world/national-security/folowing-us-indictments-chincese-military-scaled-back-hacks-on-american-industry/2015/11/30/fcdb097a-9450-11e5-b5e4-279b4501e8a6_story.html.

10 See, e.g., computer science researchers Damon McCoy, Hitesh Dharmdasani, Christian Kreibich, Geoffrey M. Voelker, and Stefan Savage's study "Priceless: The Role of Payments in Abuse-advertised Goods," https://cseweb.ucsd.edu/~voelker/pubs/priceless-ccs12.pdf.

11 David Sanger and John Markoff, "After Google's Stand on China, U.S. Treads Lightly," *New York Times,* Jan. 14, 2010; Shane Harris, "Google's Secret NSA Alliance," *Salon,* Nov. 16, 2014.

12 For some particular examples, see Shane Harris, "The Mercenaries," *Slate,* Nov. 12, 2014. For a more extensive but less concrete survey of what security firms in this field say they might do, see Amanda Craig, Scott Shackelford, Janine Hiller, "Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis," *American Business Law Journal* 52, No. 4 (2015), emphasizing emerging consensus that "active defense" may seek information but should not cause direct destruction of property not owned by the client.

13 Andrea Shalal, "Top U.S. Spy Says Skeptical about U.S.-China Cyber Agreement," Reuters, Sept. 30, 2015 (reporting on previous days' Clapper testimony before Senate Armed Services Committee), www.reuters.com/article/us-usa-cybersecurity-idUSKCN0RT1Q820150930.

14 "Local Police Grapple with Response to Cybercrimes," Associated Press, April 13, 2013, www.usatoday.com/story/news/nation/2013/04/13/local-police-response-cybercrimes/2079693/.

15 Quoted in "The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime," Police Executive Research Forum, April 2014, www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf.

16 See www.reuters.com/article/us-sony-cybersecurity-costs-idUSKBN0JN2L020141209.

17 Jeremy Rabkin and Ariel Rabkin, "Navigating Conflicts in Cyberspace: Legal Lessons from the History of War at Sea," *Chicago Journal of International Law* 14, No. 1, p. 197 (2013).

18 Grover Clark, "The English Practice with Regard to Reprisals by Private Persons," *American Journal of International Law* 27, No. 4, p. 694 (1933).

19 Of ten states with an explicit constitutional guarantee of "privacy," nine indicate that it applies only to "state action" and not to private activity. A large majority of states (thirty-seven) authorize recording or "interception" of private communications at the consent of one party to an exchange; only twelve states require consent of both parties. See Corey A. Ciocchetti, "The Privacy Bailout: State Government Involvement in the Privacy Arena," *Entrepreneurial Business Law Journal* 5, No. 2, p. 597 (2010), see pp. 607, 609, 610. On the general pattern of allowing wider data collection to private security than government policing agencies, see David Sklansky, "Private Police," *UCLA Law Review* 46, p. 1165 (1999); Jon Michaels, "Deputizing Homeland Security," *Texas Law Review* 88, p. 1435 (2010).

20 "Hat-tribution to PLA Unit 61486," June 9, 2014, CrowdStrike (available at www.crowdstrike.com/blog/hat-tribution-pla-unit-61486).

21 Mandiant, "APT1, Exposing One of China's Espionage Units," 2014 (available at intelreport.mandiant.com/Mandiant_APT1_Report.pdf).

22 Robert O'Harrow Jr., Dana Priest, and Marjorie Censer, "NSA Leaks Put Focus on Intelligence Apparatus's Reliance on Outside Contractors," *Washington Post,* June 10, 2013, www.washingtonpost.com/business/nsa-leaks-put-focus-on-intelligence-apparatuss-reliance-on-outside-contractors/2013/06/10/e940c4ba-d20e-11e2-9f1a-1a7cdee20287_story.html.

23 Available online at www.dni.gov/files/documents/SSCI_Unclassified_2016_ATA_SFR%20_FINAL.pdf.

24 Dustin Volz and Jim Finkle, "U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam," Reuters, Mar. 25, 2016, www.reuters.com/article/us-usa-iran-cyber-idUSKCN0WQ1JF.

25 Following a Washington meeting between President Obama and Chinese president Xi Jinping in September 2015, the two leaders issued a joint statement pledging that "neither the U.S. or the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property . . . or other confidential business information for commercial advantage." Skeptics noted that the Chinese seem to regard this pledge as not extending to hacking by special cyber units of the People's Liberation Army. Richard Bejtlich, "To Hack or Not to Hack?" Brookings Institution, Sept. 28, 2015, www.brookings.edu/blogs/up-front/posts/2015/09/28-us-china-hacking-agreement-bejtlich.

26 Orin Kerr, "Vagueness Challenges to the Computer Fraud and Abuse Act," *Minnesota Law Review* 94, p. 1561 (2010).

27 For example, Eugene Volokh, "The Rhetoric of Opposition to Self-Help," Volokh Conspiracy, April 11, 2007. The American Law Institute's Model Penal Code (a widely recognized guide) indicates that "the sue of force for the protection of property . . . is justifiable when . . . the actor [including a private person] believes that the person against whom he uses force has no claim to the possession of the property" (§3.06.b.11).

28 Anthony Glosson, "Active Defense: An Overview of the Debate and a Way Forward," Mercatus Working Paper, Aug. 2015, http://mercatus.org/sites/default/files/Glosson-Active-Defense.pdf.

The preferred citation for this publication is:
Jeremy Rabkin and Ariel Rabkin, **Hacking Back Without Cracking Up**, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1606 (June, 22 2016), available at http://www.lawfareblog.com/hacking-back-without-cracking.

About the Authors

JEREMY RABKIN

Jeremy Rabkin is professor of law at George Mason School of Law, where he teaches international law and administrative law. He holds a PhD in political science from Harvard University. He serves on the advisory board of the Global Internet Strategy project of the American Enterprise Institute.

ARIEL RABKIN

Ariel Rabkin is a computer scientist interested in debugging complex software systems. He has published over a dozen technical papers on topics including monitoring, configuration management, and efficient analytics. He received his PhD in Computer Science from UC Berkeley in May 2012. He is a visiting fellow at the American Enterprise Institute's Center for Internet, Communications, and Technology Policy.

Jean Perkins Foundation Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The working group's output, which includes the Aegis Paper Series, is also published on the *Lawfare* blog channel, "Aegis: Security Policy in Depth," in partnership with the Hoover Institution.

Jack Goldsmith and Benjamin Wittes are the cochairs of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams /national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION