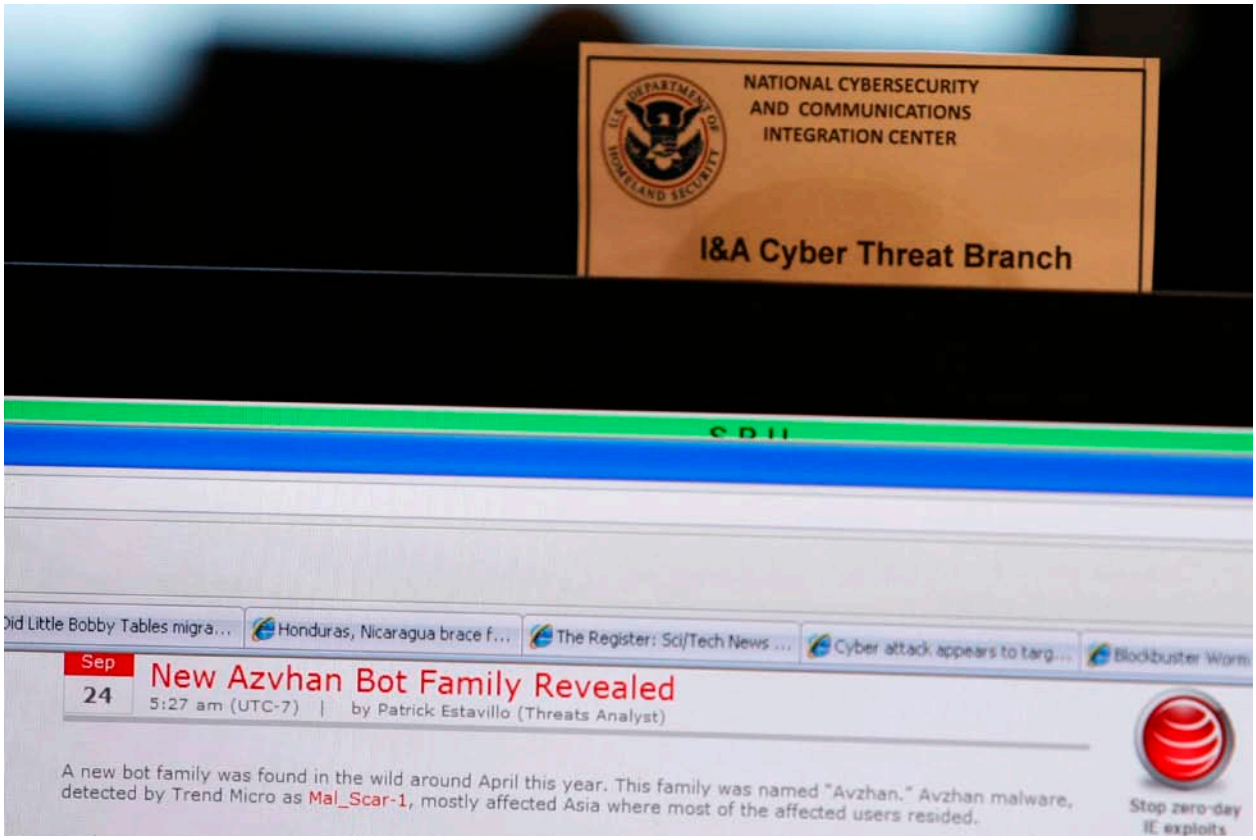
THE FUTURE OF THE CONSTITUTION

December 08, 2010



Reuters/Hyungwon Kang

The Cyberthreat, Government Network Operations, and the Fourth Amendment

Jack Goldsmith

Governance Studies at BROOKINGS

INTRODUCTION

Many corporations have intrusion-prevention systems on their computers' connections to the Internet. These systems scan the contents and metadata of incoming communications for malicious code that might facilitate a cyber attack, and take steps to thwart it. The United States government will have a similar system in place soon. But public and private intrusion-prevention systems are uncoordinated, and most firms and individual users lack such systems. This is one reason why the national communications network is swarming with known malicious cyber agents that raise the likelihood of an attack on a critical infrastructure system that could cripple our economic or military security.

Jack Goldsmith is Henry L. Shattuck Professor at the Harvard Law School; Nonresident Senior Fellow in Governance Studies, Brookings Institution; Member, Hoover Institution Task Force on Law and National Security.

To meet this threat, imagine that sometime in the near future the government mandates the use of a government-coordinated intrusion-prevention system throughout the domestic network to monitor all communications, including private ones. Imagine, more concretely, that this system requires the National Security Agency to work with private firms in the domestic communication network to collect, copy, share, and analyze the content and metadata of all communications for indicators of possible computer attacks, and to take real-time steps to prevent such attacks.

This scenario, I argue in this essay, is one end point of government programs that are already up and running. It is where the nation might be headed, though perhaps not before we first suffer a catastrophic cyber attack that will spur the government to take these steps. Such a program would be controversial. It would require congressional approval and in particular would require mechanisms that credibly establish that the NSA is not using extraordinary access to the private network for pernicious ends. But with plausible assumptions, even such an aggressive program could be deemed consistent with the U.S. Constitution, including the Fourth Amendment.

The Threat

Our economy, our energy supply, our means of transportation, and our military defenses are dependent on vast, interconnected computer and telecommunications networks that are poorly defended and inherently vulnerable to theft, disruption, or destruction by foreign states, criminal organizations, individual hackers and—potentially—terrorists. The number of public and private cyber attackers, spies, and thieves is growing rapidly. Their weapons are hidden inside the billions of electronic communications that traverse the world each day. And these weapons are becoming more potent relative to our defenses in an arena where offense already naturally dominates.[1]

[1] *See* RICHARD CLARKE AND ROBERT KNAKE, CYBERWAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT (2010); FRANK KRAMER ET AL., EDS, CYBERPOWER AND NATIONAL SECURITY (2009).

With the current state of technology, computer system defenders cannot easily determine when the systems are being attacked—at least until the attack is underway or complete, and sometimes not even then. When defenders discover the attack, the attacker's identity usually cannot quickly or precisely be ascertained. Even when the computer or geographical source of the attacks is identified, it is hard to know whether some other computer in some other place launched the attack. Even if we have certain knowledge about which computer in which place was the ultimate source of the attack, we usually do not know whether the agent behind the attack is a private party or a state actor. And even if we know the actor's geographical location and precise identity, he is usually located beyond our borders, where our law enforcement capacities are weak and where we cannot use our military power except in the most extreme circumstances. And even if we could use military force, it might not be effective in thwarting the attack in any event.

And so the mature Internet, by eliminating the geographical and physical barriers that used to protect vital American assets, has empowered untold thousands of new actors to steal or destroy these assets, and at the same time has made it difficult for the United States to find and punish, and thus deter, these actors. The result is that the U.S. government currently lacks the tools to stop the growing attacks on and theft of its vital economic and military assets. And the government is worried. President Obama thinks that the "cyber threat is one of the most serious economic and national security challenges we face as a nation." He declared in May 2009 that "our digital infrastructure—the networks and computers we depend on every day—will be treated as a strategic national asset" and the protection of this infrastructure "will be a national security priority."[2]

This most serious of national security threats presents a dilemma unique in American history. The U.S. government has access to and potential control over the channels of attack on the homeland from air, sea, land, and space. But it does not have legal access to, or potential control over, the channels of cyber attack on the homeland: the physical cables, microwave and satellite signals, computer exchange points, and the like. The private sector owns and controls these communication channels. This is a dangerous state of affairs because these private firms focus on profits, not national security, and thus tend to invest in levels of safety that satisfy their private purposes and not the national interest in cybersecurity. To make matters worse, between 90 and 95 percent of U.S. government military and intelligence communications travel over these privately owned systems—systems through which military and intelligence systems can themselves be attacked or exploited.

We have grown accustomed to thinking about computer and telecommunication systems as private communication infrastructure and about

[2] President Barack Obama, Remarks by the President on Securing on Securing Our Nation's Cyber Infrastructure (May 29, 2009) (transcript available at http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/) [hereinafter *National Archives Speech*].

data storage media as presumptively immune from government scrutiny, vigorously protected by both the Fourth Amendment and an array of complex and demanding statutory restrictions. But in the coming decades, and probably much sooner, this understanding will change, perhaps radically, because these systems are also channels of attack on our nation's most valuable military, intelligence, and economic assets. Only the government has the incentive and the responsibility to maintain network security at levels appropriate for national security. And only with the government's heavy involvement will the United States have the resources and capacity to make the network secure.

The government will need to take many politically difficult and legally controversial steps to address the cybersecurity problem. One such step, and the focus of this essay, involves the active monitoring of the private communications network. When someone enters the United States physically at the border (by air, sea, or land), or when someone physically enters a government building or a sports stadium, the government has the authority to inspect the visitor to ensure that he or she does not present a threat, and to take steps, sometimes proactive ones, to ensure that a threatening visitor does not do harm. The government asserts similar authorities at airport screening stations and highway safety checkpoints. It also asserts has the power to intercept air, sea, and land attacks on U.S. critical infrastructure components—the Twin Towers or a nuclear power plant or the banking system. The cyberthreat is no less serious than these kinetic threats, and indeed may be more serious in our wired society. Citizens will demand that the government keep these systems secure, and will punish the government if the systems are successfully attacked or exploited in ways that do serious harm. The government knows this, and it will act.

We know a bit about what the government is doing in this respect already, and what we know permits reasonable inferences about what it might try to do in the future as the cyberthreat grows and becomes more public.

The Government in the Network: What Is Happening Now

Begin with the government's little-known sensor and software system, EINSTEIN 2. This system is installed in Internet connection points between government computer systems and the public Internet. It scans a copy of all Internet traffic to and from government computers (including traffic from private parties). It then examines both the content and metadata of these copied communications for known "signatures" of malicious computer code—viruses, spyware, Trojan horses, exploitation agents, and "phishing" exploits that seek usernames, passwords, and social security numbers—that might be used to gain access to or harm a government computer system. When EINSTEIN 2 identifies a communication with a malicious signature, it automatically acquires and stores the entire message, including, for example, the content of emails. (It also deletes copied messages that do not contain a malicious signature.) The identified and stored messages are then reviewed by government officials charged with computer network defense. All of

this takes place without a warrant from a court or any other review by any party outside the Executive branch.[3]

The government is planning to supplement EINSTEIN 2, an intrusion-detection system, with EINSTEIN 3, an intrusion-prevention system. A summary of the Comprehensive National Cybersecurity Initiative ("CNCI") states that EINSTEIN 3 "will have the ability to automatically detect and respond appropriately to cyber threats before harm is done, providing an intrusion-prevention system supporting dynamic defense."[4] Former Homeland Security Secretary Michael Chertoff said that if EINSTEIN 2 is "the cop who is on the side of a road with a radar gun who can say if someone is drunk or speeding and they can phone ahead and warn that that person is coming," then EINSTEIN 3 is the cop who "make[s] the arrest" and "stop[s] the attack."[5]

EINSTEIN 3 will reportedly use "active sensors" to detect malicious attack agents and take real-time steps—most of which will be computer-automated—to prevent the attack from reaching the government system. In Chertoff's words, it "would literally, like an anti-aircraft weapon, shoot down an attack before it hits its target."[6] Many people believe EINSTEIN 3 will involve operations by the government, or by private backbone providers and Internet service providers ("ISPs") acting at the behest of the government, in private telecommunication channels (or on copies of such communications) before the malicious communication reaches or adversely affects government computers.[7]

The National Security Agency ("NSA") plays an important role in the EINSTEIN projects. NSA is America's signals-intelligence and government-information assurance agency. It is technically a component of the Department of Defense ("DoD"), and it is typically headed by a lieutenant general or vice admiral. While the NSA's collection capabilities are mostly directed outside the United

---

[3] This description of EINSTEIN 2.0 is drawn from Mem. Op. from Steven G. Bradbury, Principal Deputy Assistant Att'y Gen., to the Counsel to the President (Jan. 9, 2009), 2009 WL 3029765.

[4] *The Comprehensive National Cybersecurity Initiative*, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

[5] Brynn Koeppen, *Former DHS Sec'y Michael Chertoff says NSA's Einstein 3 is "Where We Have to Go" in Cyber Security; Calls for International Cyber Security Cooperation*, EXECUTIVEBIZ, Aug. 7, 2009, http://blog.executivebiz.com/former-dhs-secretary-michael-chertoff-says-nsa's-einstein-3-is-'where-we-have-to-go'-in-cyber-security-calls-for-international-cyber-security-cooperation/3882.

[6] *Homeland Security Seeks Cyber Counterattack System*, CNN.COM, Oct. 4, 2008, http://www.cnn.com/2008/TECH/10/04/chertoff.cyber.security.

[7] For accounts of EINSTEIN 3, *see generally Behind "Project 12,"* NEWSWEEK, Mar. 7, 2008, *available at* http://www.newsweek.com/id/119902/page/1; Ellen Nakashima, *Cybersecurity Plan to Involve NSA, Telecoms: DHS Officials Debating The Privacy Implications*, WASH. POST, July 3, 2009, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/07/02/AR2009070202771.html?wprss=rss_nation; Koeppen, *supra* note 5; Siobhan Gorman, *Troubles Plague Cyberspy Defense*, WALL ST. J., July 3, 2009, at A1, *available at* http://online.wsj.com/article/SB124657680388089139.html; Chris Strohm, *Official Says Einstein Security System Won't Read E-mails*, NEXTGOV, Oct. 15, 2009, http://www.nextgov.com/nextgov/ng_20091015_6734.php?oref=rss?zone=itsecurity; *Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace, Hearing Before the Subcomm. on Terrorism and Homeland Security of the S. Comm. on the Judiciary*, 111th Cong. (2009) (statement of Philip Reitinger, Deputy Under Sec'y, Nat'l Protection and Program Directorate, U.S. Dept. of Homeland Security), *available at* http://kyl.senate.gov/legis_center/subdocs/Reitinger.pdf.

States, NSA also has domestic responsibilities. It was the operator of the Terrorist Surveillance Program (TSP) that involved warrantless wiretapping of certain terrorist communications with one end in the United States. And it has been heavily involved in the development of the EINSTEIN systems. The Department of Homeland Security ("DHS") has stated that EINSTEIN 3 capabilities are "based on technologies developed by the NSA."[8] According to the government, the "threat signatures determined by NSA in the course of its foreign intelligence and DoD information assurance missions" will be used in the EINSTEIN system.[9] And based on threats identified by EINSTEIN 3, "alerts that do not contain the content of communications" will be sent to NSA, which will use the information to check cyber attacks in unknown ways that the government assures us are consistent with NSA's "lawfully authorized missions."[10]

NSA also has the lead in the recently established Cyber Command, which is headed by NSA Director General Keith Alexander. Cyber Command is charged with coordinating US offensive cyber activities and U.S. defensive efforts in protecting the .mil network. Consistent with the above analysis, Cyber Command is also in tasked with the responsibility of providing "support to civil authorities" in their cybersecurity efforts.[11] In addition, Deputy Secretary of Defense William Lynn recently stated that Cyber Command "works closely with private industry to share information about [cybersecurity] threats and to address shared vulnerabilities."[12]

NSA is involved with domestic cybersecurity in these and doubtlessly other ways because it possesses extraordinary technical expertise and experience, unmatched in the government, in exploring and exploiting computer and telecommunication systems. NSA also has close relationships with private telecommunications firms and other firms central to national cybersecurity.[13] These relationships are important because cybersecurity requires the government to work closely with the telecommunication firms whose hardware and software constitute the Internet's backbone and Internet connection points. These firms already have enormous experience and expertise identifying and eliminating certain types of bad actors and agents on their systems that the government leverages in stopping threats that concern it.

---

[8] *Privacy Impact Assessment for the Initiative Three Exercise*, DEPARTMENT OF HOMELAND SECURITY, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3.pdf.

[9] *The Comprehensive National Cybersecurity Initiative*, *supra* note 4.

[10] *Id*.

[11] Mem. from Robert M. Gates, U.S. Sec'y of Defense, to Secretaries of the Military Departments *et al.* (June 23, 2009), *available at* http://aviationweek.typepad.com/files/cyber-command-gates-memo1.pdf.

[12] William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, FOREIGN AFFAIRS, Sept./Oct. 2010, *available at* http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

[13] *See* SHANE HARRIS, THE WATCHERS: THE RISE OF AMERICA'S SURVEILLANCE STATE (2010); JAMES BAMFORD, THE SHADOW FACTORY: THE NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA (2009).

The Government in the Network: What Might Happen in the Future

The EINSTEIN intrusion-detection and intrusion-prevention systems are needed to protect government networks because optimal defense of these malicious attack and exploitation agents requires (among many other things) real-time traffic analysis, real-time detection, and real-time response. Many private firms (including telecommunication firms and ISPs) have intrusion-detection and intrusion-prevention systems akin to the government's EINSTEIN system. But many do not, and on the whole the government and private systems leave huge gaps in the national network, and leave it swarming with malware that can be used to do serious harm.

One solution to this broader problem is to extend the government's intrusion-prevention system to operate in the *private* communications system inside the United States.[14] Deputy Secretary of Defense William Lynn has been pushing this view of late. "We need to think imaginatively about how [the EINSTEIN 3] technology can also help secure a space on the Internet for critical government *and* commercial applications," he recently said. Private firms that refuse to opt in to such a system would "stay in the wild wild west of the unprotected internet" in ways that "could lead to physical damage and economic disruption on a massive scale."[15] Lynn later argued that "[p]olicymakers need to consider, among other things, applying the National Security Agency's defense capabilities beyond the ".gov" domain, such as to domains that undergird the commercial defense industry," and added that the Pentagon is "working with the Department of Homeland Security and the private sector to look for innovative ways to use the military's cyberdefense capabilities to protect the defense industry."[16]

At least four considerations argue for a comprehensive government-mandated, government-coordinated intrusion-prevention system throughout the U.S. network.[17] First, the government, and especially the NSA, can provide novel information about threat vectors based on its espionage and related technical capacities. Second, the government might be best positioned to coordinate different malicious signature lists generated by itself, backbone providers, ISPs, and security firms, and thus best able to create a comprehensive picture of the threat. Third, a mandatory system would fill in the significant gaps created by the many computers throughout the network that lack intrusion-detection systems. And fourth, the government has the responsibility and appropriate incentives to invest in levels of network defense appropriate for national security; private firms

---

[14] Richard Clarke proposes such a system, though he would have it strictly run by private industry. *See* Clarke, *supra* note 1.

[15] Noah Shachtman, *Cyber Command: We Don't Wanna Defend the Internet (We Just Might Have To)*, WIRED.COM (MAY 28, 2010, 9:44 AM), http://www.wired.com/dangerroom/2010/05/cyber-command-we-dont-wanna-defend-the-internet-but-we-just-might-have-to/#more-25377#ixzz0pPBH0nKB (emphasis added).

[16] Lynn, *supra* note 12.

[17] There are also many downsides, of course, some of which (privacy concerns) I discuss below, and others of which (such as the problems that adhere in a monoculture of security) I do not discuss here. For an example of the latter category of problems, *see, e.g., McAfee Anti-Virus Program Goes Berserk, Reboots PCs*, USA TODAY.COM, Apr. 21, 2010, http://www.usatoday.com/tech/news/2010-04-21-mcafee-antivirus_N.htm.

that control our information infrastructure have many technological advantages, but they lack this responsibility or these incentives. As Stewart Baker recently noted, alluding to British Petroleum's failure to invest in precautions or responses appropriate to the national interest in environmental protection: "If you like the BP spill, you'll love cyberwar."[18]

A mandatory nationwide intrusion-prevention system might place sensors at the point of entry for all communications coming into the United States, as well as at each Internet exchange point among Internet backbone providers and between the backbone providers and major cloud service providers and large private firms associated with critical infrastructure. The government itself would be involved in identifying or coordinating both the signatures that triggered intrusion in such systems and the responses to such intrusions. But it would likely work closely with the telecommunication firms whose hardware and software constitute the Internet's backbone, for these firms already have enormous experience and expertise identifying and eliminating certain types of bad actors and agents on their systems that the government will try to leverage in stopping threats that concern it.

If intrusion-prevention systems extend into the private network in this way, NSA will inevitably play an important role. As noted above, NSA already has a large role in the identification of threat signatures for EINSTEIN 3 and in the use of threat information generated by EINSTEIN 3. It is thus noteworthy that NSA is building a $1.5 billion, 1 million square foot cybersecurity data center at Camp Williams near Salt Lake City, Utah.[19] The Camp Williams facility will provide "critical support to national cybersecurity priorities" and "intelligence and warnings related to cybersecurity threats, cybersecurity support to defense and civilian agency networks, and technical assistance to the Department of Homeland Security."[20] Tasks at Camp Williams might include NSA data collection, storage, and analysis and identification of threat signatures (as with the EINSTEIN programs). Tasks may also involve government expansion of such programs into private critical infrastructure protection.

The NSA is also likely to play a role in supporting new authorities that Congress might give the President in the event of a cyber emergency. The draft Cybersecurity Act of 2009 is one example of what such an authority might look like.[21] The bill originally granted the President power to "declare a cybersecurity emergency and order the limitation or shutdown of Internet traffic to and from any compromised Federal Government or United States critical infrastructure information system or network."[22] This proposal was controversial, and a later,

---

[18] Stewart Baker, *If You Like the BP Spill, You'll Love Cyberwar*, The VOLOKH CONSPIRACY (May 29, 2009), http://volokh.com/2010/05/29/if-you-like-the-bp-spill-youll-love-cyberwar.

[19] J. Nicholas Hoover, *NSA to Build $1.5 Billion Cybersecurity Center*, INFORMATIONWEEK.COM (Oct. 29, 2009, 1:07 PM), http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=221100260.

[20] *Id.*

[21] S. 773, 111th Cong. (2009), *available at* http://www.opencongress.org/bill/111-s773/text.

[22] *Id.* at § 18(2).

more carefully worded draft granted the President, in the "event of an immediate threat to strategic national interests involving compromised Federal Government or United States critical infrastructure information systems or networks," the power to "declare a cybersecurity emergency" and, if necessary, "direct the national response to the cyber threat and the timely restoration of the affected critical infrastructure information system or network."[23]

It is unclear what this authority would entail or why it might be needed. It might mean that the President would be empowered to use existing national security resources, such as some of the NSA capabilities discussed above, to block traffic at certain locations that is destined for critical infrastructure networks, or to order backbone providers to shut down or apply certain filters at Internet connection points that happen to be "United States critical infrastructure information systems or networks" or that constitute threats to those systems or networks. One can also imagine, going even further and consonant with the speculations above, that NSA or the U.S. Computer Emergency Readiness Team ("US-CERT") would monitor all communications traffic in the United States (and elsewhere) and be authorized to examine any packet in the network that satisfies statutory criteria of a possible threat, and to order a shutdown of traffic to or from a particular IP address or provider deemed to be suspicious—all without a warrant.

Almost all of the governmental activities described above would require the significant, government-approved or government-mandated cooperation and information sharing with Internet backbone providers, ISPs, certain other communications firms, and firms related to critical infrastructure. As President Obama's Cyberspace Policy Review noted: "Network hardware and software providers, network operators, data owners, security service providers, and in some cases, law enforcement or intelligence organizations may each have information that can contribute to the detection and understanding of sophisticated intrusions or attacks. A full understanding and effective response may only be possible by bringing information from those various sources together for the benefit of all."[24]

There is already a great deal of ad hoc information sharing and coordination between the government and various industries involved in critical infrastructure concerning malicious agents, cyber intrusions, digital espionage, and the like. EINSTEIN 3, for example, is being tested with help from AT&T. Google recently requested assistance from NSA—technically under the rubric of a "cooperative research and development agreement" (CRADA)—in tracking down what happened in the alleged Chinese hack of its computers.[25] The CNCI and similar government programs contemplate coordination of government and private sector information sharing about cyberthreats to critical infrastructure on a broader and

[23] *Id.* at § 201(2).
[24] *Cyberspace Policy Review*, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
[25] John Markoff, *Google Asks Spy Agency for Help with Inquiry into Cyberattacks*, N.Y. TIMES, Feb. 4, 2010, at A6, *available at* http://www.nytimes.com/2010/02/05/science/05google.html.

more systematic basis.[26] There have been many reports of NSA's sharing classified threat information with defense contractors.[27] Extrapolating from these programs, one might expect the government to delegate many of the tasks for cybersecurity—including affirmative duties to identify, report, and eradicate malicious agents or anomalous activity on the network—to the private sector, and one might similarly anticipate the government and the private sector to have robust information-sharing arrangements.

Legal Changes

The above scenario is a nightmare for many civil libertarians: The dreaded, all-powerful, privacy-destroying, DoD-affiliated, General-run NSA, cut loose to use its giant computing and analytical powers in the homeland, in conjunction with private firms, to (a) suck up and monitor the content of private Internet communications, (b) store those communications, temporarily, (c) trace the source of malicious agents in these communications all over the globe, including inside the United States, and (d) take active steps to thwart malicious communications, even when they originate or use computers in the United States.

There is no way to know whether this scenario will come to pass. But the cyberthreat is much more serious and menacing than is generally realized. Malicious payloads are becoming ever more prevalent and ever more sophisticated, and are harder and harder to stop; our vulnerabilities are endless, and our most precious national resources are in jeopardy. It might take the "digital Pearl Harbor" that Richard Clarke predicted in 2000 for something like the steps outlined in Part III to be taken seriously and implemented, but significant losses short of a Pearl Harbor event might lead some of them to be implemented. It thus might be useful to assess, as this Part does, some of the legal hurdles the law might pose to these changes. It turns out that most of the hurdles are statutory and thus can be changed by Congress. The biggest constitutional hurdle is the Fourth Amendment, and, at the end of the day, the Fourth Amendment does not present as much of a hurdle to the program sketched above as one might expect.

Non-Constitutional Issues

The main change necessitated by the scenario in I have described would be legislation to significantly alter the complex patchwork of mostly outdated restrictions on the government's ability to collect and analyze the content and meta-data of communications in the homeland or involving Americans. "This patchwork exists," noted President Obama's Cyberspace Policy Review, "because, throughout the evolution of the information and communications infrastructure,

[26] *Behind "Project 12,"* NEWSWEEK, Mar. 7, 2008, *available at* http://www.newsweek.com/id/119902/page/1.
[27] Shane Harris, *The Cyber Defense Perimeter*, NAT'L J., May 2, 2009, *available at* http://www.nationaljournal.com/njmagazine/id_20090502_5834.php.

the Federal government enacted laws and policies to govern aspects of what were very diverse industries and technologies."[28]

Most of these laws—including FISA, the Wiretap Act, and the Stored Communications Act—were written at a time when the idea of cyber attacks on critical infrastructure was inconceivable. And most would need to be revised, along three broad dimensions. First, Congress would need to clearly authorize the President, with some modicum of particularity, to take the affirmative steps outlined. Second, it would need to authorize the government to mandate the cooperation of private firms, as described above, to monitor the network, collect and analyze content and meta-data in the network, and take proactive steps to meet cyberthreats. And, third, it would need to implement various mechanisms of accountability and review, some of which I outline below.

One quasi-constitutional objection to the scheme I have outlined is that the military under the guise of the NSA would be active in the homeland. This certainly raises significant political concerns. But no fundamental legal barrier stands in the way of such an arrangement. Beyond the Third Amendment's prohibition on quartering of soldiers in private homes in peacetime without compensation, the Constitution places no bar on military activity in the homeland. The main source of constraint on homeland military activity is the Posse Comitatus statute, which prohibits, "except in cases and under circumstances expressly authorized by the Constitution or Act of Congress," the willful use of "any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws."[29] The Posse Comitatus law reflects the strong sub-constitutional norms against military involvement in homeland security, but for several reasons it does not prohibit NSA from assuming an aggressive domestic cybersecurity role.[30] First, Posse Comitatus is probably not implicated by the imagined NSA activity because such activity does not contemplate the execution of the laws. Second, its prohibitions by its own terms can be altered by statute. Congress has enacted many exceptions to its ban, and can do so again.

A second quasi-constitutional objection concerns the involvement of private firms in domestic cybersecurity. In the scheme envisioned here, many front-line cybersecurity tasks—both in identifying threats and responding to them—are performed by private Internet backbone operators and ISPs. Again, there are many serious policy concerns here. One is ensuring that private firms are subject to carrots and sticks that induce them to have the proper incentives to perform U.S. national cybersecurity tasks. A second and related concern is that many of the most consequential private firms in this area (such as Verizon and AT&T) have a global presence (including in places like China), and are doubtless under analogous pressures from other countries to help with cybersecurity tasks. Delicate steps must be taken to ensure that these foreign entanglements do not

[28] *Cyberspace Policy Review*, *supra* note 25.
[29] 18 U.S.C. § 1385.
[30] For an outstanding overview, *see* William O. Scharf, Cybersecurity, Cybercommand, and the Posse Comitatus Statute, 2010 (unpublished manuscript) (on file with author).

jeopardize private cybersecurity cooperation with the U.S. government, or that such cooperation does not, through private firms, end up serving the national security goals of our adversaries. There is also the related and very tricky problem that global consumers might not want to use the services of information technology firms that actively participate in cybersecurity efforts with the U.S. government, for fear the U.S. government would be more likely to monitor their communications. These are all formidable policy concerns that are beyond the scope of this essay. None of them, however, presents a fundamental legal bar to private involvement in national security. Indeed, for better or worse, the vast majority of U.S. defense and intelligence budgets are spent on private contractors.

The Fourth Amendment

The Fourth Amendment presents the most significant constitutional hurdle to the cybersecurity regime I have outlined. The Fourth Amendment's fundamental prohibition is on "unreasonable searches and seizures." It also requires that all warrants issued in support of a search or seizure be reasonable. But the Fourth Amendment does not require a warrant in impractical circumstances as long as the search or seizure is reasonable under the circumstances. The courts may not see the Fourth Amendment today as permitting the unfathomably massive copying, storage, and analysis of private communications I have described above—though, having not confronted a sufficiently similar question yet, they have never written anything controlling that would preclude such actions either. But if the national and economic security threat of cyber attacks comes to be viewed as sufficiently severe and sufficiently difficult to stop, then government steps like those outlined here, properly authorized and limited in ways proportionate to the task, could easily be deemed reasonable under the circumstances, which is all the Fourth Amendment ultimately requires.

The doctrinal building blocks for this conclusion are already in place. Begin with the metadata that would be collected and analyzed. Metadata includes the "to" and "from" addressing information for e-mails, IP addresses of visited Web sites, routing information that tracks a communication's path on the Internet, and possible traffic volume information. It is pretty well settled that there is no reasonable expectation of privacy in such information and thus that the government collection and analysis of such information does not implicate the Fourth Amendment.[31] Only statutes stand in the way, and these statutes can be amended.

The collection (or copying) and analysis of bulk communication content is constitutionally more controversial, but the doctrinal tools for permitting it are already in place as well. One such doctrinal tool can be found in what Christopher Slobogin, in his contribution to this series, describes as a "series of cases holding

[31] *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979); *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 904-05 (9th Cir. 2008); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008).

that people assume the risk that information disclosed to third parties will be handed over to the government and thus cannot reasonably expect it to be private." Another doctrinal tool, and the one I will focus on here, is the Fourth Amendment's "special needs" doctrine.

The special needs doctrine establishes an exception to the Fourth Amendment warrant requirement for reasonable governmental actions with a purpose that goes "beyond routine law enforcement and insisting upon a warrant would materially interfere with the accomplishment of that purpose."[32] The doctrine requires courts to consider and weigh a number of public and private interest factors, discussed below. It has been used to uphold warrantless, non-law-enforcement searches without individualized suspicion in numerous contexts, including highway checkpoint stops, random drug testing, searches of government employees with dangerous jobs, and inspections of regulated businesses. It has also been used, more directly on point, to uphold various suspicionless, terrorism-related searches. Consider two examples.

The first involves a suspicionless vehicle and carry-on baggage search on ferries on Lake Champlain. In an opinion by then-Judge Sotomayor, the Second Circuit ruled that defendants' undiminished expectations of privacy in bags and cars were outweighed by the government's interest in searching these items, based on an analysis of (a) the character and degree of the government intrusion, (b) the nature and immediacy of its needs, and (c) the efficacy of its policy in addressing those needs. On the first point, the court ruled that the brief duration of the search, advance notice of the search, and the responsible manner in which the search was conducted made the degree of intrusion on the privacy right minimal. On the second point, it ruled that "[p]reventing or deterring large-scale terrorist attacks presents problems that are distinct from standard law enforcement needs and indeed go well beyond them."[33] Relying on *Von Raab*,[34] a landmark drug-testing case, and airport search cases, the court noted that that the government "need not adduce a specific threat in order to demonstrate a 'special need'" and that "in its attempt to counteract the threat of terrorism, [it] need not show that every airport or every ferry terminal is threatened by terrorism in order to implement a nationwide security policy that includes suspicionless searches."[35] Finally, the court concluded that the searches in question were reasonably effective because they were reasonably calculated to deter potential terrorists.

The second example comes from *In re Directives*, a case from the United States Foreign Intelligence Surveillance Court of Review. The court was considering the legality of a government foreign intelligence surveillance order to a private

---

[32] In re Directives [redacted text] Pursuant to Section 1058 of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1009 (FISA Ct. Rev. 2008) (*quoting* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995)); O'Connor v. Ortega, 480 U.S. 710, 725 (1987) (plurality opinion); *id.* at 732 (Scalia, J., concurring); Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 665-66 (1989); Griffin v. Wisconsin, 483 U.S. 868, 872 (1987).

[33] Cassidy v. Chertoff, 471 F.3d 67 (2d Cir. 2006).

[34] *Von Raab*, 489 U.S. 656.

[35] *Cassidy*, 471 F.3d at 83.

communications service provider pursuant to the temporary (and now-expired) 2007 Amendments to FISA. The 2007 statute authorized the Director of National Intelligence and Attorney General to authorize the acquisition of foreign intelligence information concerning persons "reasonably believed to be outside the United States," as long as five safeguards were employed.[36] Analogizing to the "special needs" cases, the court concluded that there was a "foreign intelligence exception" to the warrant requirement. The court first reasoned that no warrant was needed because the "programmatic purpose" of the surveillance was gathering foreign intelligence, not law enforcement, and because "requiring a warrant would hinder the government's ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake." It then concluded (based on the totality of the circumstances) that the surveillance was reasonable and thus did not violate the Fourth Amendment, because the governmental interest (national security) was of "the highest order" and a "matrix of safeguards"—including techniques designed to be directed against foreign powers, and well as minimization (privacy-protecting) procedures—adequately protected legitimate private interests.[37]

The cybersecurity efforts envisioned here are significantly broader than the searches in either of these two cases. But the logic of these cases applies pretty straightforwardly to the cybersecurity situation. As top government officials, including the President, have all made clear, the nation's most vital resources are "severely threatened" by cyber attacks and cyber exploitations.[38] The purpose behind the cybersecurity collection and analysis scheme would not be law enforcement but rather the protection of the critical infrastructure that undergirds our military and economic security. For a nationwide intrusion-detection system to have a chance at legality, the government, backed by express congressional findings, would need to establish that (a) network-wide coverage is necessary because deadly computer attack agents are tiny needles hidden inside giant haystacks consisting of billions of innocent communications that each day travel at the speed of light and are often designed to learn from computer defense systems—automatically and at computer speed—and morph to exploit their vulnerabilities; and (b) only comprehensive, speed-of-light collection and analysis will enable the government to find and thwart this threat and keep the network and the infrastructure connected to it safe.

A Model for Constitutional Cybersecurity Surveillance

The strong need for a nationwide intrusion-detection system, the non-law enforcement purpose of the system, and the impracticability of a warrant would help the government skirt the warrant requirement for domestic cybersecurity

[36] 50 U.S.C. § 1805b (2007).
[37] In re Directives [redacted text] Pursuant to Section 1058 of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1013 (FISA Ct. Rev. 2008).
[38] *National Archives Speech*, *supra* note 2.

activities only if they are reasonable under the totality of the circumstances. It is impossible to say what is reasonable without a concrete sense of the severity of the cybersecurity threat and the precise measures the government will take to meet it. One can speculate very generally that if the public perceives the threat to be severe enough to induce Congress and the President to take some of the steps I have outlined, and if these steps are implemented with adequate safeguards that ensure that the broad searches are conducted in ways proportionate to the task, it would likely survive a constitutional challenge. A useful model for such safeguards, and for a broader scheme of legitimating checks and balances, can be found in the innovative reforms in the FISA Amendments Act of 2008, which replaced the 2007 amendments at issue in the 2007 FISC appellate case.[39]

The 2008 reforms reaffirmed the 2007 power of the DNI and AG to authorize, without a warrant, "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[40] But it included four fundamental checks (some of which were present in the 2007 law) that inform the reasonableness of searches under this authority. First is a requirement for an *independent ex ante scrutiny* by the Foreign Intelligence Surveillance Court (FISC) that results in a certification that the government's general targeting procedures are reasonably designed to stay within statutory guidelines.[41] Second and perhaps most important are various *privacy and Fourth Amendment-protecting requirements*, most notably "minimization procedures" that are themselves subject to ex ante review and approval by the FISC. Third are a variety of *ex post oversight mechanisms*: The AG and the DNI must assess legal compliance and report to Congress every six months, and inspectors general across the intelligence community and DOJ must perform annual reviews for legal compliance and effectiveness.[42] Fourth, the 2008 law contains a 2012 *sunset provision* that requires Congress to revisit and reapprove (if it so desires) the entire scheme after four years of operation.

These four "programmatic" mechanisms would inform the proportionality and reasonableness of the scheme and could form the foundation of any aggressive government cybersecurity activity in the domestic network.

Independent Ex Ante Scrutiny

The NSA (or, more likely, NSA working in conjunction with another agency, like DHS) might be required to seek prior independent approval for the basic procedures it uses both in collecting or copying masses of communications, and in identifying the malicious signatures and other computer or telecommunication anomalies that its intrusion-detection and intrusion-prevention and related

[39] FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436.
[40] 50 U.S.C. §1881a(a).
[41] *Id*. at (i)(3).
[42] *Id*. at (l)(3).

systems pick out and redress. This independent approval might come from the FISA court or a FISA-type court created just for this purpose. Such an ex ante check would ensure that the general collection criteria are proportionate and reasonable. It would provide general congressional sanction and executive implementation subject to an ex ante global judicial approval of the reasonableness of the system in achieving the congressional aim.

Privacy-Protecting Mechanisms

Concrete mechanisms to protect privacy and to ensure that the government's search is minimally intrusive and reasonably efficacious will be central to any Fourth Amendment special-needs analysis. It is hard to be specific about what this might entail without knowing the specifics of the program in question or the details of particular searches. But the following factors would be relevant under the special needs cases.

First, if the logic of the EINSTEIN 3 program is applied to the private network, then private Internet communications will be copied and searched by machines for malicious signatures, and then copied communications that contain no malicious signatures—the vast bulk of copied communications—will be destroyed. If this works as planned, then the vast bulk of the intrusions on privacy are temporary and no human being will ever see communications without known signatures. Moreover, communications that are identified as containing malicious signatures might have reduced expectations of privacy under the line of cases holding that a search technique that reveals only illegal activity does not infringe on legitimate expectations of privacy.[43] These cases are suggestive and not directly on point because many and maybe most communications that contain malicious agents will do so inadvertently or negligently, and thus will not (at least under the law as it stands now) be illegal.

Second, the government could place significant use restrictions on the communications identified as containing malicious signatures. The government would not be precluded from using criminal information found in a special-needs, non-law enforcement search as part of a criminal investigation or trial. But to demonstrate the narrowness and reasonableness of the search and to minimize the chilling effect on communications, the government might limit what it can do with the filtered communications that are presumptively threatening to national security. It might, for example, create a tiered response—from least invasive (such as stripping off the malicious code) to most intrusive (destroying the communication)—to communications containing malicious signatures. And it might limit the criminal uses to which presumptively threatening communications can be put—for example, by limiting the use of such communications in a specified

[43] *See, e.g.,* United States v. Jacobsen, 466 U.S. 109 (1984) (chemical field test that reveals only whether white powder is cocaine infringes on no legitimate expectation of privacy); United States v. Place, 462 U.S. 696, 706-07 (1983) (sniff by a police dog trained to detect narcotics was not a "search" under the Fourth Amendment).

list of computer-related or national security crimes.

Third, the intrusion-prevention system would require a variety of minimization procedures to ensure that (among other things) (a) communications identified as false positives are immediately destroyed and (b) communications that match threat signatures are examined in ways that do not reveal any more private information than is necessary to meet the threat. In this context, the government might develop what John Poindexter during his Total Information Awareness days called "privacy appliances"—software devices that automatically filter out or encrypt all non-essential private information in communications examined by human beings.[44] The government could also employ David Brin's strategy of snooping on itself to ensure that it does not go further than necessary in snooping on its citizens.[45] It could, for example, record all relevant individual government official computer activities and establish credible, immutable log and auditing trails that permit ex post auditing and investigation of what government officials were doing with its access to citizen communications.

Extensive Ex Post Auditing

Broad government network operation would also have to be checked by a number of ex post auditing and reporting requirements. Senior leaders would have a duty to certify effectiveness and abuse to Congress. And inspectors general would have a duty to audit the program for effectiveness and abuse and report the results to the Executive branch and Congress. These ex post requirements would influence official behavior ex ante.

Sunset Provision

A sunset provision is a useful and now-frequently used tool in the context of novel national security challenges. We still have relatively little information about the aims and capacities and threats posed by cyber enemies, and we have little information on how any government network activity will work in practice, or what effect it will have on liberty and security. Congress should thus force itself to revisit the design and operation of the system in a few years, after more information becomes available.

Conclusion

Without a warrant or particularized suspicion, U.S. citizens are forced through invasive screening procedures at U.S. airports, sports events, and courthouses. Citizens' laptops, mail, and luggage are also checked at the border and at the

[44] *See* Harris, *supra* note 13; *see also* K.A. Taipale, *Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd*, 7 YALE J. L. & TECH. 123, 179-197 (2004).
[45] DAVID BRIN, THE TRANSPARENT SOCIETY (1998).

entrances to critical infrastructure components and other sites attractive to terrorists. We allow such warrantless searches because the government's order and security interests are high and the searches reasonable and proportionate to the task. Analogous searches for analogous reasons on masses of domestic communications seem untoward because of the number of communications involved and because we do not think bits of data or strings of code can do much harm. But bits and strings can do, and are doing, enormous harm, and there might be little way for the government to check this harm short of having a comprehensive picture of what is happening in the network. In such a world, massive government snooping in the network can be lawful if proper and credible safeguards are put in place.

Thanks to Orin Kerr, Larkin Reynolds, and Jeffrey Rosen for conversations and comments, and Matthew Bobby, Keith Gerver, and Joshua Gruenspecht for research assistance and related help. This work was funded by the Office of Naval Research under award number N00014091059. The opinions, conclusions, and recommendations expressed are mine alone and do not necessarily reflect the views of the Office of Naval Research.

Jack Goldsmith is the Henry L. Shattuck Professor at Harvard Law School, where he teaches and writes about national security law, presidential power, cybersecurity, international law, internet law, foreign relations law, and conflict of laws. Before coming to Harvard, Professor Goldsmith served as Assistant Attorney General, Office of Legal Counsel from 2003-2004, and Special Counsel to the Department of Defense from 2002-2003.

Governance Studies
The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
www.brookings.edu/governance.aspx

Editor
Jeffrey Rosen
Benjamin Wittes

Production & Layout
John S Seo

E-mail your comments to gscomments@brookings.edu