Atlantic Council

BRENT SCOWCROFT CENTER
ON INTERNATIONAL SECURITY

ISSUEBRIEF

BY FRANKLIN D. KRAMER AND MELANIE J. TEPLINSKY

Cybersecurity and Tailored Deterrence

DECEMBER 2013

Cyber has become the new conflict arena. It ranks as one of the greatest national security challenges facing the United States for three reasons. First, as the revelations about the National Security Agency's (NSA's) activities suggest, cyber offense has far outpaced cyber defense. Second, cyber capabilities are prevalent worldwide and increasingly are being used to achieve the strategic goals of nations and actors adverse to the United States. Third, it is highly unlikely that cyber espionage and other cyber intrusions will soon cease. While the NSA disclosures focus on the United States and the United Kingdom, there is little doubt that China, Russia, Iran, North Korea and others are engaged in significant cyber activities. The fundamental question is whether the cyber realm can, consistent with the national interest, be made more stable and secure.

This paper proposes that a critical step in the establishment of such a stable and secure cyber space will be the development of a tailored deterrence approach to cyber that reduces the national security threat from cyberadversaries. Tailored deterrence will not be sufficient in and of itself to stabilize and secure cyberspace. For example, it will not resolve fundamental issues—laid bare by the reaction to the NSA revelations—regarding the relationship of the US government to its citizens and companies as well as to its close allies. Norms of behavior and requirements of law will need to be reviewed. But tailored deterrence can serve as a key element of a cybersecurity strategy designed to reduce adversarial intrusion into US private, commercial, and governmental networks.

Despite over a decade of US government and private sector investment in network defenses designed to reduce our vulnerability to cyber intrusion,

Cyber Statecraft Initiative

The Atlantic Council's Cyber Statecraft Initiative helps foster international cooperation and understanding of new forms of competition and conflict in cyberspace through global engagement and thought leadership.

the two key national security threats from cyber adversaries—cyber espionage and cyberattack against critical infrastructure—are increasingly severe. Evidence of this trend includes mounting reports of ongoing nation-state sponsored campaigns of intellectual property (IP) theft against major US corporations and defense industrial base companies;[1] the escalating spate of attacks on US financial institutions over the past two years;[2] and the 2012 cyberattack against Saudi Aramco—one of the most destructive attacks on the private sector to date—which destroyed over 30,000 computers at the world's largest energy company.[3]

Neutralizing the cyber threat will take more than redoubled efforts to defend our networks. Hardening

1 Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace* (2011), http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf; Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (February 2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

2 See Nicole Perlroth, "Attacks on 6 Banks Frustrate Customers," *New York Times*, September 30, 2012, http://www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html; Chris Strohm and Eric Engleman, "Cyber Attacks on U.S. Banks Expose Vulnerabilities," *Businessweek*, September 28, 2012, http://www.businessweek.com/news/2012-09-27/cyber-attacks-on-u-dot-s-dot-banksexpose-computer-vulnerability.

3 Siobhan Gorman & Julian A. Barnes, "Iran Blamed for Cyberattacks: U.S. Officials Say Iranian Hackers Behind Electronic Assaults on U.S. Banks, Foreign Energy," *Wall Street Journal*, Oct. 12, 2012, http://online.wsj.com/article/SB10000872396390444657804578052931555576700.html.

Franklin D. Kramer is a distinguished fellow and member of the board at the Atlantic Council and a former assistant secretary of defense for international security affairs. **Melanie J. Teplinsky** is on the Advisory Board for CrowdStrike, Inc., is an Adjunct Professorial Lecturer at American University's Washington College of Law, and previously counseled on cybersecurity while in private practice at Steptoe & Johnson LLP.

networks certainly will prevent some attacks, but it will not prevent them all. It is not only the NSA which has significant cyber capabilities, and a defense-only strategy will fail against nation-state actors and other determined adversaries who have the time, motivation, and resources to defeat even sophisticated defenses. Moreover, if history is any guide, a defense-only cyber strategy is unsustainable in the long-term because it will saddle US government and private organizations with escalating costs for enhanced—but ultimately imperfect—network defenses that adversaries will defeat for a fraction of the cost.

For these reasons, this paper recommends that the United States shift from a defense-only paradigm to a hybrid model of cybersecurity based not only on defense, but also on tailored deterrence, with a heavy emphasis on raising the costs of, and reducing the benefits from, cyber attacks. Tailored deterrence can be a key part of a strategy to provide a stable, secure cyber space. This paper provides a brief overview of the concept of tailored deterrence and recommends the following four critical actions designed to increase attacker costs, deny attackers the benefits of their attacks, mitigate key consequences, and extend the breadth of those efforts into the international arena so we need not "look back years from now and wonder why we did nothing in the face of real threats to our security and our economy":[4]

1. **Cyber Sanctions:** Authorize both governmentally imposed sanctions for cyber espionage and civil remedies, including treble damages and forfeiture, in order to deter cyber threat actors by imposing costs, or the threat thereof.

2. **Certified Active Defense:** Authorize a limited number of certified private entities to work with government to take active defense measures focused on attribution, initially to protect critical information within the defense industrial base. Active defense measures directed toward attribution will deter adversaries by raising the costs and risks associated with cyber espionage.

3. **Focused Standards for Protection and Resilience—Electric Grid and Finance:** Reduce critical infrastructure vulnerability and enhance resilience by developing differentiated mandatory standards, initially for the most critical electric power and financial companies. Reducing vulnerability bolsters our defenses and increasing resilience enhances deterrence by mitigating the consequences of any successful intrusions.

4. **Agreement Among Like-minded Nations:** Expand protection against espionage and critical infrastructure vulnerability via agreement among like-minded nations. Common international approaches can extend and amplify deterrent effects and could be achieved initially through agreement among the United States, Australia, Canada, France, Germany, Japan, the Republic of Korea, the United Kingdom, and perhaps the European Union, to create a Cyber Stability Board.

Because several of these recommendations involve new approaches, this paper proposes that they be undertaken on a pilot-program, or other limited basis, which can be evaluated and expanded if proven effective and desirable.

To maximize their effectiveness, these recommendations can and should be implemented in tandem while maintaining the United States' drive for an open Internet and its commitment both to preserve and enhance personal privacy and to protect civil liberties. None of the recommendations above implicates any of the programs made public in the recent revelations of the activities of the National Security Agency (NSA), but privacy and civil liberty considerations should still be reviewed in connection with their adoption and implementation.

1. Tailored Deterrence

Tailored deterrence recognizes that adversary calculations can be affected by more than the threat of simple retaliation through attack. Increasing costs to adversaries through methods other than attack as well as denying adversaries the benefits of an attack (e.g., "deterrence through denial"), including through consequence mitigation, can have significant deterrent effects on an adversary and should be utilized as part of an effective cybersecurity strategy.

Tailored deterrence most clearly entered official United States doctrine in the 2006 *Quadrennial Defense Review* (QDR),[5] though, of course, elements of the analysis had long been part of strategic thought. The

4 Barack Obama State of the Union Address, supra note 1.

5 The QDR discussed a "shift from a 'one size fits all' notion of deterrence toward more tailorable approaches appropriate for advanced military competitors, regional WMD states, as well as nonstate terrorist networks." See US Department of Defense, *Quadrennial Defense Review Report* (2006), http://www.defense.gov/qdr/report/Report20060203.pdf.

concept has since regularly been reaffirmed[6] including in the President's 2012 strategic defense review which provides that "[c]redible deterrence results from both the capabilities to deny an aggressor the prospect of achieving his objectives and from the complementary capability to impose unacceptable costs on the aggressor."[7]

Tailored deterrence previously has been applied to asymmetric warfare issues in a manner that has application to cyber. In a 2012 analysis of tailored deterrence and terrorism, Matthew Kroenig and Barry Pavel wrote:

> Deterrence is a strategic interaction in which an actor prevents an adversary from taking an action that the adversary otherwise would have taken by convincing the adversary that the cost of taking that action will outweigh any potential gains. To achieve deterrence, therefore, an actor can shape the adversary's perception of the costs or benefits of a particular course of action...
>
> When considering deterrence, many analysts think solely in terms of deterrence-by-retaliation, but deterrence theorists also advanced a second type of deterrence strategy: benefit denial, or deterrence-by-denial, strategies which contribute to deterrence by threatening to deny an adversary the benefits of a particular course of action. . . . If actors believe that they are unlikely to succeed or reap significant benefits from a certain course of action, they may be deterred from taking it.[8]

Kroenig and Pavel make clear that while defense and deterrence by denial overlap, there is an important distinction:

> Deterrence is distinct from other strategies such as defense. There is a fine line between deterrence-by-denial and defense because defensive postures can have deterrent effects and deterrent capabilities can aid in a defensive operation. To distinguish between these approaches, we follow previous scholarship in defining defensive policies as those that are designed primarily to fend off an opponent in the event of an attack, and deterrence policies as those that are intended to convince an adversary not to attack in the first place.[9]

In the discussion below, deterrence theory is applied to cyber in nontraditional manners; that is, by raising costs through other than threat of attack and by denying the benefits of cyber attack to adversaries. Such actions would not encompass the full spectrum of a cyber strategy, however. There still are reasons for strong defenses and, in the context of actual warfare, the threat of retaliation. The discussion herein, however, significantly broadens cyber strategy by making deterrence a feasible effort short of all-out retaliation.[10]

2. Cyber Sanctions

The United States has long utilized sanctions against individuals, entities, and countries in pursuit of counterterrorism, nonproliferation, and other policies. Cyber sanctions could be used in a comparable fashion to meet the growing challenge of cyber industrial espionage. Cyber sanctions will deter cyber espionage by raising costs, or the threat thereof, and therefore are essential to the broader cybersecurity strategy recommended in this paper.

Cyber sanctions would have three critical benefits to the United States. First, they would raise the cost to malicious hackers.[11] Second, they would send a strong geopolitical signal to countries that encourage or actively support malicious hacking. Third, if done properly, they could authorize and encourage private initiatives, which would then supplement

6 US Department of Defense, *Deterrence Operations: Joint Operating Concept, Version 2.0* (December 2006), www.dtic.mil/futurejointwarfare/concepts/do_joc_v20.doc.

7 US Department of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (January 2012), http://www.defense.gov/news/defense_strategic_guidance.pdf.

8 Matthew Kroenig and Barry Pavel, "How to Deter Terrorism," *Washington Quarterly* (Spring 2012), 22-23.

9 Ibid., 23.

10 Among others, Stewart Baker, former Assistant Secretary for Policy at the Department of Homeland Security, has discussed the potential role of deterrence in cybersecurity, including elements of a tailored deterrence strategy. Testimony of Stewart A. Baker, *Hearing on The Department of Homeland Security at 10 Years: Examining Challenges and Achievements and Addressing Emerging Threats* before the Senate Committee on Homeland Security and Governmental Affairs, 113th Congress 6-8, September 11, 2013. See also Stewart Baker, "The Attribution Revolution," *Foreign Policy*, June 17, 2013, http://www.foreignpolicy.com/articles/2013/06/17/the_attribution_revolution_plan_to_stop_cyber_attacks#sthash.L1y53aPb.dpbs.

11 Zachary K. Goldman, "Washington's Secret Weapon Against Chinese Hackers," *Foreign Affairs*, April 18, 2013, http://www.foreignaffairs.com/articles/139139/zachary-k-goldman/washingtons-secret-weapon-against-chinese-hackers.

the government's capability to respond to malicious hacking.

Sanctions could be of two types. They could be governmental, akin to nonproliferation or counterterrorism sanctions,[12] or they could provide civil remedies, which would be a new approach.

Governmental sanctions could be implemented by the President under existing law, or new authorities could be created by the Congress. Under existing law, the President already has the authority to impose targeted sanctions against cyber threat actors. Specifically, under the International Emergency Economic Powers Act (IEEPA),[13] the President can declare a "national emergency" where there is an "unusual or extraordinary [foreign] threat" to the United States' "national security, foreign policy, or economy."[14] The President would then have broad authority under the IEEPA to address the cyber threat through financial sanctions, including freezing the US-based assets of, and blocking financial transactions with, individuals, private organizations, and governments contributing to the threat.[15] The already substantial effect of these actions would be amplified by the fact that financial institutions throughout the world "often refuse to do business with sanctioned entities."[16]

Alternatively, Congress could establish a cyber sanctions regime through legislation. Two separate bills currently are pending. The Senate bill, the Deter Cyber Theft Act (DCTA),[17] requires the President to block imports of products containing or similar to stolen US technology or made or exported by a company that the director of national intelligence identifies as having benefited from theft of US technology or proprietary information.

The House bill, the Cyber Economic Espionage Accountability Act (CEEAA),[18] requires the President to identify—and make public (unless inconsistent with national security)—a list of foreign government officials or agents stealing IP via cyber espionage. Under CEEAA, such persons would be ineligible for US visas and would be listed on the Office of Foreign Assets Control's Specially Designated Nationals and blocked persons list. Moreover, CEEAA authorizes the President to exercise all authorities granted under IEEPA to freeze the assets of such persons.

Cyber sanctions also profitably could be extended by providing civil remedies to corporate victims of cyber espionage. One of the differences between cyber and other areas is the significant economic impact on private entities. General Keith Alexander, head of US Cyber Command, recently characterized the volume of IP theft that the United States experiences as "astounding"[19] and publicly stated that, in his opinion, it is the "greatest transfer of wealth in history,"[20] although more recent analysis has reduced the probable size of the loss.[21] Given that situation, authorizing private entities to seek legal remedies against malicious hacking entities could be beneficial.

As a general matter, 'private attorneys general' support public policy ends in many arenas. Empowering private sector cyber espionage victims to seek monetary damages could substantially raise the costs of, and

12 See, e.g., http://www.state.gov/r/pa/prs/ps/2013/02/204013.htm. See also Department of State, Bureau of Nonproliferation, Imposition of Nonproliferation Measures on an Entity in China, Including a Ban on U.S. Government Procurement, 68 Fed. Reg. 28314 (May 23, 2003). Similar actions simultaneously were taken with respect to Iran's Shahid Hemmat Industrial Group. See Department of State, Bureau of Nonproliferation, Imposition of Nonproliferation Measures on an Iranian Entity, Including a Ban on U.S. Government Procurement, 68 Fed. Reg. 28315 (May 23, 2003).

13 IEEPA, 50 U.S.C. §§ 1701-07.

14 Ibid. § 1701.

15 Ibid. § 1702(a). See Baker, "The Attribution Revolution," supra note 12.

16 Goldman, supra note 11.

17 The bill was introduced by Senators Jay Rockefeller (D-WV), John McCain (R-AZ), Carl Levin (D-MI), and Tom Coburn (R-OK). See Deter Cyber Theft Act, S. 884, 113th Cong. (2013), http://www.gpo.gov/fdsys/pkg/BILLS-113s884is/pdf/BILLS-113s884is.pdf.

18 The bill was introduced in the House by Representatives Mike Rogers (R-MI) and Tim Ryan (D-OH). See Cyber Economic Espionage Accountability Act, H.R. 2281, 113th Cong. (2013), http://beta.congress.gov/113/bills/hr2281/BILLS-113hr2281ih.pdf.

19 General Keith Alexander, "Cyber Security and American Power," YouTube video, 51:00, posted by US Military, July 11, 2012, http://www.youtube.com/watch?v=nTwiZneMw3U. Note Alexander's remarks at 34:30.

20 Ibid. at 09:06-09:11. Dmitri Alperovitch, chief technology officer at CrowdStrike, Inc. and senior fellow with the Cyber Statecraft Initiative at the Atlantic Council, appears to have coined this phrase in August 2011 while working as vice president of threat research at McAfee, Inc. According to Alperovitch, "What we have witnessed over the past five to six years has been nothing short of a historically unprecedented transfer of wealth—closely guarded national secrets (including those from classified government networks), source code, bug databases, email archives, negotiation plans and exploration details for new oil and gas field auctions, document stores, legal contracts, supervisory control and data acquisition (SCADA) configurations, design schematics, and much more has 'fallen off the truck' of numerous, mostly Western companies and disappeared in the ever-growing electronic archives of dogged adversaries." See Dmitri Alperovitch, McAfee, Inc., *Revealed: Operation Shady Rat* (2011), http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

21 James A. Lewis and Stewart A. Baker, Center for Strategic and International Studies and McAfee, *The Economic Impact of Cybercrime and Cyber Espionage* (July 2013), http://csis.org/publication/economic-impact-cybercrime-and-cyber-espionage.

thereby deter, cyber espionage. A private attorneys general approach potentially would have significant value if affected firms were allowed to collect punitive damages, perhaps treble damages, as in antitrust suits or specified statutorily authorized damages for circumstances in which the specific determination of compensatory damages would be difficult.

The viability of a 'private attorneys general' approach rests, in part, on successful attribution. The private sector has made great strides in addressing the attribution problem, which generally was viewed as intractable just a few short years ago. Effective attribution via nongovernment sources is now possible in at least some cases, as evidenced by the February 2013 Mandiant Report,[22] which offered extensive evidence—including actual video of intrusion activities[23]—of the role that China's People's Liberation Army played in a years-long cyber espionage campaign against companies in the United States. This capability paves the way for private litigants to obtain meaningful remedies for cyber espionage.

Several potential avenues exist for private litigants to obtain civil remedies for cyber espionage. First, the EEA could be amended to include a federal civil cause of action for economic espionage, including (1) treble damages for any losses arising out of economic espionage; and (2) a statutory penalty and/or a civil forfeiture provision. The availability of treble or statutory damages would encourage victimized corporations to sue EEA violators, redounding to the nation's benefit.

While a judicial remedy could be useful, an alternative would be to utilize an administrative proceeding in which government would both expedite and support private claims for loss/damage from cyber espionage and cyber attacks. Private and governmental efforts could be combined as is done in the government contracting context when a contractor initiates a bid protest challenging the propriety of a contract award. To initiate a proceeding, a private entity would file its claim with an administrative body of the government, just as bid protests are filed with the Government Accountability Office. The government then would be responsible for reviewing all evidence (classified and unclassified) in its possession and preparing for the private litigant an unclassified "report" including such evidence. After any necessary administrative adjudication to resolve disputed issues of fact or law, the record would be complete, and the administrative agency would issue a decision. If the agency determines that a foreign government or foreign actor was responsible for the cyber espionage or cyber attack that the private litigant alleged, administrative sanctions could be imposed on those entities. This would be new ground but given the magnitude of the cybersecurity problem, such an approach is worthy of serious consideration.

Once a private litigant has obtained a judgment against a foreign actor, a civil forfeiture provision should be an integral part of any statutory remedy. Such a provision would give the courts the authority to order the seizure of property used to commit, facilitate or owned by a company benefitting from the commission of the violation. Seizure of a foreign actor's property offers a way to attack the economic base of cyber threat actors.

A second enforcement mechanism would be to block imports of products benefitting from cyber espionage, as proposed in the Senate bill referenced above. This would provide relief in the competitive arena and also generate grounds for the offending entity to change its practices and settle with the harmed party.

Sanctions should not be looked on as a panacea in and of themselves as they generally are most effective as part of a comprehensive effort.[24] Sanctions—both governmental and through private attorneys general—would, however, raise adversaries' costs of engaging in cyber attacks and, in conjunction with the steps

22 Mandiant, supra note 1.

23 The video shows live APT1 Chinese threat actors conducting computer network espionage activities. See "APT1: Exposing One of China's Cyber Espionage Units," YouTube video, 5:00, posted by MandiantCorp, February 18, 2013, http://www.youtube.com/watch?v=6p7FqSav6Ho.

24 As Sue Eckert and Thomas Biersteker argue, "[t]argeted sanctions tend to be most effective when they are well-designed, well-coordinated with other diplomatic initiatives, and consistently implemented by major trading and commercial partners over an extended period of time. International political resolve ("political will") is also critically important to their success... Targeted sanctions never work in isolation from other policy instruments—be they ongoing negotiations, unilateral or regional sanctions measures, independent activities of international organizations, or the activities of other UN agencies." See Sue Eckert and Thomas Biersteker, Canada Department of Foreign Affairs and International Trade, International Security Research and Outreach Programme, *The Impacts and Effectiveness of UN Nonproliferation Sanctions: A Provisional Report on the Targeted Sanctions on Iran and North Korea* (2012), http://www.international.gc.ca/arms-armes/assets/pdfs/Report-CCDP_Sanctions.pdf. See also Rocky Cole, "Nonproliferation and Economic Sanctions in American Grand Strategy," Roosevelt Institute/Campus Network blog, April 4, 2010, http://www.rooseveltcampusnetwork.org/blog/nonproliferation-and-economic-sanctions-american-grand-strategy.

outlined below, could play a pivotal role in the effort to address the growing cyber threat. [25]

3. Certified Entities and Active Defense

For over a decade, the cornerstone of US cybersecurity policy has been vulnerability mitigation—strengthening cyber defenses to reduce vulnerability to attack. But there is a growing understanding that defense—particularly in the face of concerted adversaries focused on a specific target—will be most successful if it includes "active" components that serve a deterrent function, beyond passive protection alone. Accordingly, this paper recommends limited active defense measures as one element of a broader deterrence-based strategy.

Active defense received its first significant notice when the Department of Defense (DoD) published its 2011 strategy for operating in cyberspace.[26] Although the term "active defense" is not specifically defined in the DoD cyber strategy, it has since been associated with a broad spectrum of activities.[27]

This article is not advocating broad authorization for the private sector to engage in active defense, concerns about which have been spelled out in detail elsewhere,[28] nor is it advocating private sector retaliation, vigilantism, or hackback. Rather, this paper recommends, as a starting point, authorizing those limited active defense measures that contribute to better (1) assurance (including better detection of intrusions and malicious activity across the supply chain); and (2) attribution (i.e., identification of threat actors). Such measures will raise adversaries' costs and risks, thereby serving a deterrent function essential to the success of the proposed hybrid cybersecurity model.

A new legal framework authorizing *certified* private sector cybersecurity providers to take limited, but meaningful steps under proper supervision likely would be an important element of tailored deterrence. A way to begin would be to create a framework to help protect the nation's most significant secrets maintained in the defense industrial base. Such a framework would set forth the requirements for "certification," and would require cybersecurity providers to meet certain standards, register with the government, and/or satisfy bonding requirements. To ensure adequate oversight, transparency, and accountability, the legal framework also would require certified cybersecurity providers to describe in advance and subsequently report their participation in certain activities to law enforcement. The use of private actors in such situations has a strong historical basis.[29]

Such efforts would need to be carefully constrained. The economic and political ramifications of the use of certain active defense techniques on globally interconnected networks may require the type of judgments that governments ordinarily make. Moreover, engaging in active defense potentially implicates US domestic law at both the federal and state levels, and, given the global reach of the Internet and cyber adversaries, active defense may involve actions or effects outside US borders, potentially implicating the domestic law of other nations. On the other hand, a limited number of entities certified by the government in their expertise and working with government could add to the government's capabilities to address extensive cyber intrusions through the application of active defense. Such certified private sector entities acting under government supervision could be authorized to take limited steps to capture the attribution evidence necessary to raise the costs to—and thereby deter—cyber adversaries whether through sanctions, civil litigation, criminal prosecution, or a "name and shame" strategy. [30]

25 Ibid.

26 US Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (2011), http://www.defense.gov/news/d20110714cyber.pdf.

27 These include watermarking IP, beaconing, using honeypots, sinkholing, using deception, retrieving stolen IP, and programming stolen IP to self-destruct. Beacons have been described as "digital dye packs" and have been likened to the well-known "Lo Jack" system used to track stolen vehicles. Honeypots are "decoy systems designed to lure intruders to a controlled environment from which to observe their behavior." See Kim Peretti and Todd McClelland, "Legal Issues with Emerging Active Defense Security Technologies," Alston & Bird LLP, January 11, 2013, http://www.alston.com/Files/Publication/c638c36f-0293-45fa-ba20-ee50b12e00fe/Presentation/PublicationAttachment/4a6feb1e-c091-4352-977c-d45bcd114d3c/Cyber-Alert-legal-issues-with-emerging-active-defense-security-technologies-1-11-13.pdf. Sinkholing is redirecting the malware on an infected computer to communicate not with the adversary's command and control server, but instead with a "safe" server controlled by "good guys." Sinkholing is a pro-active measure that can be used to respond to the adversary by wresting botnet-infected computers from cyber adversaries' control. Finally, deception includes allowing adversaries to steal "fake" data (e.g., fake bidding strategies) in order to raise adversaries' costs. This broad spectrum of active defense measures can be used to (1) detect malicious activity; (2) trace/pursue/identify the adversary and any stolen IP; (3) raise adversaries' costs through interference, delay, or obstruction; and (4) respond to the adversary (e.g., by recovering stolen IP).

28 James A. Lewis, *Private Retaliation in Cyberspace*, Center for Strategic and International Studies, 2013, http://csis.org/publication/private-retaliation-cyberspace.

29 U.S. Const. art. I, § 8, cls. 10-11 (authorizing letters of marque).

30 See Baker Testimony, supra note 10 at 7-8 (suggesting using the private sector to investigate cyber intrusions, with government-set limits and oversight) and Baker, "The Attribution Revolution," supra note 12 (discussing the role of the private sector in identifying and "naming and shaming cyberspies").

Finally, recognizing that even the best-regulated program potentially could result in harm to innocent third parties, the proposed legal framework should provide for government compensation if authorized active defense measures cause such harm. Such a framework would permit a limited group of certified private sector actors to engage, with oversight, in socially beneficial actions while ensuring the availability of compensation should innocent actors suffer any damage as a result.

4. Focused Standards for Protection and Resilience—Electric Grid and Finance

Cyber standards also have a potentially important role to play in the proposed hybrid model of cybersecurity. Cyber standards could be of significant value if clearly delineated and made mandatory in limited sectors where the public interest is very substantial.[31] Standards should focus not only on protection, but also on resilience, since it cannot be assumed that networks will not be penetrated. Resilience, by denying the benefits of an attack, would have deterrent impact, as would stronger defenses in the arenas where an adversary could potentially create the most harm to the nation.

In the cyber arena, most firms' evaluation of risks generally coincides with the national risk. However, in the case of key critical infrastructures — particularly electricity and finance — that certainly is not the case. For example, the harm from the loss of electric power, especially for an extended time, goes far beyond one firm's loss of revenue. Duke Energy, PG&E Corporation, and other major electric power firms are in a different category than, by comparison, Walmart or Ford Motor Company or Pizza Hut. This is equally true for major banks and financial institutions.

Accordingly, mandatory standards could be limited to a very few key critical infrastructures — as suggested, a good starting point would be electric power and finance — and only the most significant entities in those fields. It probably makes sense to start initially only with the largest companies in each field, say no more than the top 50 and perhaps fewer. Those firms would have the capacity to implement mandatory standards and their experience could provide a model for others. It would further make sense, and indeed only be fair, to expect those firms to receive compensation for the cost of implementing the standards since the requirements would be mandatory for the national interest, not for market reasons.

An important question regarding mandatory standards is whether standards can be clearly delineated.[32] In fact, there are a series of fundamental actions that would greatly improve cybersecurity. On the protection side, it would be entirely possible to create a standard that required patching within forty-eight hours, whitelisting, use of least privilege, and continuous monitoring. These are equivalent to the so-called "Australian top 4," which the Australian government has publicly stated could have mitigated at least 85 percent of the targeted cyber intrusions to which its Defence Signals Directorate responded in 2010.[33] Other well-known and effective measures include programming in so-called "safe languages," using operational systems with limited capabilities, encryption of key data streams, and authentication with cryptography.

Enhanced protection, while highly desirable, cannot immunize operational systems against penetration. Resilient systems are therefore necessary. Standards that enhance resilience will not prevent an attack but will improve our ability to mitigate the consequences

31 As James A. Lewis argues, "[t]he basic problem—true since 1998—is there are no incentives sufficient to make companies in most critical infrastructure sectors take voluntary action to bring the security of their networks to the level needed for national defense. Congress could fix this if it ... [gave] the federal government the ability to mandate compliance with reasonable standards when this is needed to defend the nation"). See James A. Lewis, "Code Red," *Foreign Policy*, August 1, 2012, http://www.foreignpolicy.com/articles/2012/08/01/code_red. See also James A. Lewis, *Raising the Bar for Cybersecurity* (2013), http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf, 7-10 (discussing the benefits of implementing the "Australian top 4").

32 One criticism of the Federal Energy Regulatory Commission-approved North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards for the bulk power system (available at http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx) and of NERC's proposed CIP Version 5 Standards is that organizations may have difficulty implementing and certifying compliance with the standards due to lack of clarity. See Notice of Proposed Rulemaking, Version 5 Critical Infrastructure Protection Reliability Standards, 143 FERC ¶ 61,055 at 2-4, 6 https://www.ferc.gov/whats-new/comm-meet/2013/041813/E-7.pdf ("[W]e believe that...certain aspects of the [proposed CIP version 5 Standards] raise concerns regarding the potential ambiguity and, ultimately, enforceability of the [standards]....[W]e are concerned that... [certain] language [in the proposed CIP version 5 Standards] is unclear with respect to the compliance obligations it places on regulated entities and that it is too vague to audit and enforce compliance.... Reliability Standards with unclear requirements or lacking minimum controls can create uncertainty and erode an otherwise effective cyber security posture.").

33 Australia Department of Defence, Defence Signals Directorate, "Strategies to Mitigate Targeted Cyber Intrusions," October 2012, http://www.dsd.gov.au/publications/Top_35_Mitigations_2012.pdf. See also, Lewis, "Raising the Bar," supra note 38 at 1 ("DSD found that four risk reduction measures block most attacks. Agencies and companies implementing these measures saw risk fall by 85 percent and, in some cases, to zero.").

of successful attacks, and therefore play an important role in the proposed hybrid cybersecurity strategy.

While a good deal of analytic work has been done on resilience,[34] there are far too few actual capabilities available. A two-pronged approach is required. Longer-term, a significant research and development effort needs to be undertaken. More immediately, resilience can be enhanced through integrity, segmentation, and the capacity to fight back and regain control of infected networks.

Integrity capabilities exist in the market and essentially allow a potentially infected network to be reset to a known status. Requiring electric power control networks and key financial networks to have that capacity is important. Segmentation dissociates certain parts of the network from others, thereby helping isolate sources of infection. Segmentation could be complemented by redundancy — not of complete networks but of key portions. Fighting back to regain network control can be necessary if the intruder seeks to keep out the network operator, which is potentially likely in a significant conflict. Fighting back will require human efforts: highly-trained "white hat counterhackers." Generating such teams could be a combined government-private sector effort. Much as the government provides some key elements in disaster relief and other elements come from the private sector, government funding and training could help create and support underlying capabilities that take advantage of private sector human capital and organization. One approach might be a "Cyber Guard" modeled on the National Guard but which could allow some greater private sector organizational efforts.

None of these proposed remedies is perfect, of course, just as no set of standards can protect against accidents or failures in other arenas. What they can do, however, is make things significantly better. In brief, there is a short list of well-known approaches that would have high value for cybersecurity. All of these could be included in a cyber standard.

Of course, it is important not to "freeze" bad solutions into regulations. One of the primary concerns associated with mandatory regulatory regimes is that "imposing rigid regulatory requirements—requirements that by their nature will be unable to keep up with rapidly evolving technologies and threats—would require industry to focus on obsolete security requirements rather than facing the actual threat at hand, effectively making systems less secure."[35] A mandatory regulatory regime for limited sectors could be designed to ameliorate such concerns. Regulations could focus on outcomes and companies could be left with the freedom to choose the technologies used to achieve those outcomes. To prevent companies from focusing on compliance with "obsolete" regulatory requirements, companies could be deemed to comply with regulations when they achieve an outcome equal to, "or better" than, that specified in the regulations.

In short, mandatory cyber standards limited to key critical infrastructure would allow a focused effort that takes account of national interest beyond that which the market alone would generate and are therefore an important element of the hybrid cybersecurity strategy described herein.

5. Like-minded Nations

The Internet is structurally and operationally international, and it would seem to follow that cybersecurity would be enhanced through cooperation among like-minded nations.[36] There already have been some steps including the Budapest Convention, which is focused on cyber crime; some coordination through military and other security arrangements such as in NATO; and more generalized discussions in fora such as the Association of Southeast Asian Nations (ASEAN) Regional Forum (ARF), the Asia-Pacific Economic Cooperation Organization (APEC), and the Organization for Economic Cooperation and Development (OECD).[37]

What has not yet happened, however, is an effectively coordinated effort to deal with cyber espionage and critical infrastructure vulnerability to prevent serious

34 See, e.g., Harriet G. Goldman, *Building Secure, Resilient Architectures for Cyber Mission Assurance*, Mitre Corporation, 2010, http://www.mitre.org/publications/technical-papers/building-secure-resilient-architectures-for-cyber-mission-assurance.

35 See Telecommunications Industry Association, *Securing the Network: Cybersecurity Recommendations for Critical Infrastructure and the Global Supply Chain,* 2012, http://tiaonline.org/sites/default/files/pages/TIACybersecurityWhitePaper_0.pdf.

36 See Bob Butler and Irving Lachow, "Multilateral Approaches for Improving Global Security in Cyberspace" in "International Engagement on Cyber: 2012," special issue, *Georgetown Journal of International Affairs* (2012):10-12, http://journal.georgetown.edu/special-issue-cyber/international-engagement-on-cyber-2012/.

37 White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

economic and national security consequences[38] for the United States and its close partners. A significant attack on electric power, telecommunications, or finance could have very consequential economic results not only for the country being attacked but also for its economic partners. Likewise, on the security side, militaries are heavily dependent on electricity, telecommunications and finance to maintain their operational effectiveness. Allies and close partners that expect to work together and rely upon one another have an interest not only in their own cyber systems but also those of their allies and partners.

An international entity dealing with both espionage and critical infrastructure vulnerability would be of great value. For example, a "Cyber Stability Board, along the lines of the financial stability board established by nations for financial issues under the Basel agreements, could be created."[39] Nations that could effectively do this include Australia, Canada, France, Germany, Japan, the Republic of Korea, the United Kingdom, the United States, and perhaps the European Union.

There is no likelihood of creating such a board unless the issues presented by the NSA revelations focusing on spying among countries are resolved in some satisfactory form. As is well-known, the United States has a "Five Eyes" agreement with the United Kingdom, Canada, Australia, and New Zealand concerning espionage. The countries named above that are not included in the Five Eyes—France, German, Japan and the Republic of Korea—are all close treaty allies of the United States. It should be possible to organize a common approach to espionage—both military and industrial—and cyber security with such countries since each is a full democracy with common interests. To be sure, there would have to be changes in behavior, not only on the United States' part but also by others—for example, there are numerous media reports of French industrial espionage. On balance, the gains from a common approach to cyber security appear to outweigh any significant loss from curtailing espionage especially given the close working relationships generally found among these countries.

Assuming that the geopolitical obstacles to creating such a board could be surmounted, such a board could coordinate multiple international cybersecurity efforts, increasing defenses and enhancing deterrence. First, focusing on cyber espionage, nations could establish governmental cyber sanctions along the lines suggested above. As noted, sanctions work best as part of a coordinated effort, including on an international level, and the board could help develop common approaches to sanctions.

Second, the board could facilitate common approaches to the use of active defense by certified private sector actors. Certified actors would be more effective if operating under a common international legal regime. As noted above, creating a legal regime that allows private entities to engage in limited active defense measures focused on attribution may require significant legal changes. Coordinating multiple national laws would be a task for the board.

Third, the board could help develop a coordinated operational approach. Cooperative action by like-minded nations—including sharing data, analysis, and tools concerning threats and remediation, as well as undertaking combined operations—could significantly enhance the operationalization of self-defense and resilience efforts.

Fourth, in order to ensure that militaries can operate as required, common standards should be established between and among this group of like-minded countries for key critical infrastructures upon which militaries depend. All of these nations are treaty allies with the United States and have worked closely on multiple military standards-setting activities. Ensuring that there is good coordination between military requirements and civilian run cyber structures could be a function of the board.

Fifth, international agreement could help enhance effective public-private partnerships. The involvement of private entities is at a minimum very valuable and often indispensable to cybersecurity. As has previously been recommended,

> One key element will be to create a network of strategic decision-makers—including from the private sector—who could be identified in advance to deal with attacks on critical infrastructure. There is no virtue in having an ad hoc approach to such a significant problem,

38 According to the Commission on the Theft of American Intellectual Property, cyber espionage is "having a devastating effect on U.S. economic interests." See The Commission on the Theft of American Intellectual Property, *The Commission Report on the Theft of American Intellectual Property* (2013), http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

39 Franklin D. Kramer, *Achieving International Cyber Stability*, Atlantic Council, 2012, http://www.acus.org/publications/reports/achieving-international-cyber-stability.

and organized procedures would be of great value.[40]

An international approach also would benefit critical infrastructure providers, many of which operate on a multinational basis.

Sixth, while it would not be the only place to do so, a board could harmonize national approaches to the key cyber offenders. A common front to the intrusions will enhance the effectiveness of response.

Seventh, an international board could harmonize privacy and civil liberty approaches. These issues are raised clearly in both international and domestic terms by the NSA revelations. While, as this article has suggested, the United States, along with its allies, has the opportunity to fundamentally shift the odds in its favor in the long-running cyber fight, that needs to be done while preserving the commitment to innovation, an open Internet, personal privacy, and the protection of civil liberties.

There are clear differences in approach to privacy and civil liberties in the transatlantic context and, more generally, among the United States and its allies. Those considerations need to be dealt with, and while our recommendations do not implicate personal privacy in most instances, data privacy may come into play to the extent that Internet Service Providers (ISPs) and/or private cybersecurity providers in the course of network monitoring collect data that could be considered personally identifiably information. In these instances, ISPs and other private companies should be required to handle (e.g., collect, use, disclose) such information consistent with the fair information practice principles, and appropriate oversight/accountability measures should be in place to ensure that any monitoring system is used in the way promised; that appropriate data destruction/retention policies are in place; and that information is not misused (e.g., improperly shared with government or shared in violation of stated privacy policies).

Finally, it should be recognized that a deterrence approach is not necessarily a one-way street. Nations adversely affected by cyber sanctions or other deterrence measures designed to curb economic espionage can take steps of their own to respond. As will be recalled, in the Cold War it was "mutual" assured destruction. While mutuality is not likely to be the case, it would not be impossible to expect China, for example, which states that it is the object of significant international cyber intrusions, to create a mirror-like regime (or even an asymmetric response) to deal with such activities (likely with less due process). Policymakers would need to evaluate this prospect, but the overall benefit of an organized international approach to creating a more stable, secure cyberspace appears to counsel strongly in favor of undertaking the steps recommended above.[41]

Conclusion

Cybersecurity is of fundamental concern to the United States and its allies and partners, but there is no silver bullet. To achieve the necessary degree of security, it is imperative to reject a defense-only cyber strategy and embrace a hybrid strategy that relies not only on defense but also on tailored deterrence to reduce overall cyber risk. Toward this end, this paper recommends simultaneously raising the costs to cyber offenders; increasing the private sector's ability to complement the government's efforts to achieve security; and developing standards and other approaches that focus on resilience as well as protection, take into account the international nature of cyber, and simultaneously are fair to companies on whom additional burdens are placed. Through the targeted actions described in this issue brief, all of these goals can be achieved and a more secure cyberspace created.

40 Ibid. at 12.

41 Testimony of James A. Lewis, *Statement Before the House Energy and Commerce Committee on Oversight and Investigations: Cyber Espionage and the Theft of U.S. Intellectual Property and Technology* (July 9, 2013) at 9.

Atlantic Council Board of Directors

INTERIM CHAIRMAN
*Brent Scowcroft

PRESIDENT AND CEO
*Frederick Kempe

VICE CHAIRS
*Robert J. Abernethy
*Richard Edelman
*C. Boyden Gray
*Richard L. Lawson
*Virginia A. Mulberger
*W. DeVier Pierson
*John Studzinski

TREASURER
*Brian C. McK. Henderson

SECRETARY
*Walter B. Slocombe

DIRECTORS
Stephane Abrial
Odeh Aburdene
Peter Ackerman
Timothy D. Adams
John Allen
*Michael Ansari
Richard L. Armitage
*Adrienne Arsht
David D. Aufhauser
Elizabeth F. Bagley
Ralph Bahna
Sheila Bair
Lisa B. Barry
*Rafic Bizri
*Thomas L. Blair
Julia Chang Bloch
Francis Bouchard
Myron Brilliant
*R. Nicholas Burns
*Richard R. Burt
Michael Calvey
James E. Cartwright
Ahmed Charai
Wesley K. Clark
John Craddock
David W. Craig
Tom Craren
*Ralph D. Crosby, Jr.
Thomas M. Culligan
Nelson Cunningham
Ivo H. Daalder
Gregory R. Dahlberg
*Paula J. Dobriansky
Christopher J. Dodd
Conrado Dornier
Patrick J. Durkin
Thomas J. Edelman
Thomas J. Egan, Jr.
*Stuart E. Eizenstat
Julie Finley
Lawrence P. Fisher, II
Alan H. Fleischmann
Michèle Flournoy
*Ronald M. Freeman
*Robert S. Gelbard
*Sherri W. Goodman
*Stephen J. Hadley
Mikael Hagström
Ian Hague
Frank Haun
Rita E. Hauser
Michael V. Hayden
Annette Heuser
Marten H.A. van Heuven
Marillyn Hewson
Jonas Hjelm
Karl Hopkins
Robert Hormats
*Mary L. Howell
Robert E. Hunter
Wolfgang Ischinger
Deborah James
Reuben Jeffery, III
Robert Jeffrey
*James L. Jones, Jr.
George A. Joulwan
Stephen R. Kappes
Maria Pica Karp
Francis J. Kelly, Jr.
Zalmay M. Khalilzad
Robert M. Kimmitt
Henry A. Kissinger
Peter Kovarcik
Franklin D. Kramer
Philip Lader
David Levy
Henrik Liljegren
*Jan M. Lodal
*George Lund
*John D. Macomber
Izzat Majeed
Wendy W. Makins
Mian M. Mansha
William E. Mayer
Eric D.K. Melby
Franklin C. Miller
*Judith A. Miller
*Alexander V. Mirtchev
Obie L. Moore
*George E. Moose
Georgette Mosbacher
Bruce Mosler
Thomas R. Nides
Franco Nuschese
Sean O'Keefe
Hilda Ochoa-Brillembourg
Ahmet Oren
Ana Palacio
Thomas R. Pickering
*Andrew Prozes
Arnold L. Punaro
Kirk A. Radke
Joseph W. Ralston
Teresa M. Ressel
Jeffrey A. Rosen
Charles O. Rossotti
Robert Rowland
Stanley O. Roth
Harry Sachinis
William O. Schmieder
John P. Schmitz
Anne-Marie Slaughter
Alan J. Spence
John M. Spratt, Jr.
James Stavridis
Richard J.A. Steele
James B. Steinberg
*Paula Stern
John S. Tanner
Peter J. Tanous
*Ellen O. Tauscher
Karen Tramontano
Clyde C. Tuggle
Paul Twomey
Melanne Verveer
Enzo Viscusi
Charles F. Wald
Jay Walker
Michael F. Walsh
Mark R. Warner
J. Robinson West
John C. Whitehead
David A. Wilson
Maciej Witucki
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
David C. Acheson
Madeleine K. Albright
James A. Baker, III
Harold Brown
Frank C. Carlucci, III
Robert M. Gates
Michael G. Mullen
William J. Perry
Colin L. Powell
Condoleezza Rice
Edward L. Rowny
James R. Schlesinger
George P. Shultz
John W. Warner
William H. Webster

LIFETIME DIRECTORS
Carol C. Adelman
Lucy Wilson Benson
Daniel J. Callahan, III
Kenneth W. Dam
Lacey Neuhaus Dorn
Stanley Ebner
Edmund P. Giambastiani, Jr.
John A. Gordon
Barbara Hackman Franklin
Robert L. Hutchings
Chas W. Freeman
Carlton W. Fulford, Jr.
Roger Kirk
Geraldine S. Kunstadter
James P. Mccarthy
Jack N. Merritt
Philip A. Odeen
William Y. Smith
Marjorie Scardino
William H. Taft, IV
Ronald P. Verdicchio
Carl E. Vuono
Togo D. West, Jr.
R. James Woolsey

**Members of the Executive Committee*
List as of September 23, 2013

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

1030 15th Street, NW, 12th Floor, Washington, DC 20005
(202) 778-4952, AtlanticCouncil.org