MERCATUS
RESEARCH

WHY THE CYBERSECURITY FRAMEWORK WILL MAKE US LESS SECURE

Eli Dourado and Andrea Castillo

MERCATUS CENTER
George Mason University

Bridging the gap between academic ideas and real-world problems

ABOUT THE MERCATUS CENTER AT GEORGE MASON UNIVERSITY

The Mercatus Center at George Mason University is the world's premier university source for market-oriented ideas—bridging the gap between academic ideas and real-world problems.

A university-based research center, Mercatus advances knowledge about how markets work to improve people's lives by training graduate students, conducting research, and applying economics to offer solutions to society's most pressing problems.

Our mission is to generate knowledge and understanding of the institutions that affect the freedom to prosper and to find sustainable solutions that overcome the barriers preventing individuals from living free, prosperous, and peaceful lives.

Founded in 1980, the Mercatus Center is located on George Mason University's Arlington campus.

www.mercatus.org

Mercatus Center at George Mason University
3434 Washington Boulevard, 4th Floor
Arlington, VA 22201
(703) 993-4930
mercatus.org

Release date: April 17, 2014

ABOUT THE AUTHORS

Eli Dourado is a research fellow in the Technology Policy Program at the Mercatus Center at George Mason University. He specializes in Internet governance, intellectual property, political economy, and the economics of technology. His writing has appeared in the *New York Times*, the *Washington Post*, *Foreign Policy*, the *Guardian*, *Ars Technica*, and *Wired*, among other outlets.

In 2012, Dourado cocreated the International Telecommunication Union transparency site WCITLeaks.org and participated in the World Conference on International Telecommunication as a member of the US delegation. Along with WCITLeaks cocreator Jerry Brito, he won an IP3 award from Public Knowledge in 2013 for his contributions on Internet governance.

Dourado is a PhD candidate in economics at George Mason University and received his BA in economics and political science from Furman University.

Andrea Castillo is a research associate at the Mercatus Center at George Mason University focusing on economic and technology policy. She is pursuing a PhD in economics at George Mason University. She is a coauthor of *Liberalism and Cronyism: Two Rival Political and Economic Systems* with Randall G. Holcombe and *Bitcoin: A Primer for Policymakers* with Jerry Brito. She received a BS in economics and political science from Florida State University.

ABSTRACT

The "Cybersecurity Framework" is an ambitious plan to federally categorize industries and prioritize vulnerabilities as determined by federal agencies and private consultants. Cybersecurity Framework proponents believe this federally designed, initially voluntary set of standards can improve cybersecurity for protected firms and industries that the Department of Homeland Security designates as "critical infrastructure sectors." In reality, much of the functioning Internet governance that users enjoy today is not a product of government committees but rather a natural emergence from the rules and incentives that permeate the Internet, called "dynamic cybersecurity." What is more, the Cybersecurity Framework is likely to cause more problems than it solves. This paper describes dynamic cybersecurity provision, contrasts this with the shortcomings of the Cybersecurity Framework, and proposes better reforms to improve dynamic cybersecurity provision for critical infrastructure.

JEL codes: O380, H12, H560

Keywords: cybersecurity, Cybersecurity Framework, network security, Internet, Internet governance, insurance, data breach, technology policy, dynamism, emergence, security, cyberwar

Amid the twin dramas of international cyber spying and mass domestic surveillance, policymakers and analysts are attempting to develop solutions to perceived cybersecurity vulnerabilities. The current lack of centrally designed and centrally enforced standards has prompted some policymakers and commentators to conclude that adequate cybersecurity protections do not exist.[1] They worry that barriers to adopting such protections prevent key stakeholders of our "critical digital infrastructure" from widely sharing the best existing cybersecurity practices.[2] Building on the Clinton and Bush administrations' early steps in identifying and prioritizing this perceived vulnerability,[3] President Obama initiated a voluntary national cybersecurity program, originally titled the "Cybersecurity Framework," through Executive Order 13636.[4]

---

1. A report from the Center for Strategic and International Studies (CSIS) is representative: "It is undeniable that an appropriate level of cybersecurity cannot be achieved without regulation, as market forces alone will never provide the level of security necessary to achieve national security objectives." See CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency* (December 2008), http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.
2. Michael Daniel, "Incentives to Support Adoption of the Cybersecurity Framework," *White House Blog*, August 6, 2013, http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.
3. The US Critical Infrastructure Protection Program was created by the Clinton administration in 1998. Later presidential directions called upon federal agencies to further identify and prioritize the protection of critical infrastructure. These initiatives were later given legislative backing with the Homeland Security Act of 2002. See Bill Clinton, "Critical Infrastructure Protection," Presidential Decision Directive/NSC-63, May 22, 1998, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm; and George W. Bush, "Critical Infrastructure Identification, Prioritization, and Protection," Homeland Security Presidential Directive 7 (HSPD-7), Department of Homeland Security website, December 17, 2003, http://www.dhs.gov/homeland-security-presidential-directive-7.
4. "Improving Critical Infrastructure Cybersecurity," Executive Order 13636, part III, 78 Fed. Reg. 33 (February 12, 2013), http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf. The final draft of the framework, released on January 12, 2014, changed the title to the "Framework for Improving Critical Infrastructure Cybersecurity." We will use the shorter term "Cybersecurity Framework" to refer to the final draft released on January 12, 2014, in keeping with Executive Order 13636. See National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

Contrary to these officials' concerns,[5] the lack of a single, central cybersecurity standard does not automatically imply a lack of adequate cybersecurity. In fact, private actors already have intrinsic incentives to develop cybersecurity solutions in the absence of a central plan. Although harder to detect than codified standards, emergent market- and norm-based standards are more robust, effective, and affordable than state-directed alternatives. Contrary to Director of National Intelligence James Clapper's contentions that these cyber threats "cannot be overstated,"[6] the likelihood of feared "cyber doom" scenarios is also much lower than policymakers believe.[7] Although popular tracts have played upon fears to justify expanded government control of the Internet, many of the threats presented are hypothetical, spurious, and often poorly substantiated.[8] Dramatic cyber doom scenarios easily capture the public's attention, but private and public resources should focus on realistic problems, like data breaches and cyber espionage.

Proposed policy solutions for this problem, such as the Cybersecurity Framework, trade emergent resilience of the Internet for opaque control of it. Policymakers run the risk of undermining the spontaneous, creative sources of experimentation and feedback that drive Internet innovation. This paper will describe the current dynamic provision of cybersecurity and explain how a technocratic solution like the Cybersecurity Framework could weaken this process and ultimately undermine cybersecurity.

DYNAMIC CYBERSECURITY PROVISION

How has the Internet worked so far in the absence of a unified cybersecurity plan? For decades, businesses, consumers, and organizations have managed to safely

5. "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," *White House Policy Review*, May 8, 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

6. James R. Clapper, "Worldwide Threat Assessment," Testimony to the House Permanent Select Committee on Intelligence, April 11, 2013, http://www.dni.gov/files/documents/Intelligence%20Reports/HPSCI%20WWTA%20Remarks%20as%20delivered%2011%20April%202013.pdf.

7. Sean Lawson, "Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History" (Mercatus Center Working Paper No. 11-01, Mercatus Center at George Mason University, Arlington, VA, January 2011), http://mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidence-history_1.pdf.

8. The best seller *Cyber War*, for instance, laments, "How do you convince someone that they have a problem when there is no evidence you can give them?" Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2012), 123. Much of the book details hypothetical threats, but most of the concrete breaches the authors identify are "primitive" DDoS attacks. See Clarke and Knake, *Cyber War*; see also Mike McConnell, "How to Win the Cyber-War We're Losing," *Washington Post*, February 28, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html.

transact, communicate, and collaborate online with few major disruptions.[9] The Internet is a dynamic, open-ended system that operates under predictable rules and encourages dispersed individuals to apply their creativity and enterprise to generate cybersecurity solutions in unpredictable ways. These solutions are a product of the "informal, trust-based relationships among the Internet operational community members," in the words of Internet governance scholar Milton Mueller.[10] When we examine some of these relationships, we will see that "most of the actual work is done not by national states promulgating and enforcing public law, but by private actors in emergent forms of peer production, network organizations, and markets."[11]

The Internet is a network of networks. Network operators do their best to provide reliable and comprehensive access to their users. Universities, companies, and Internet service providers (ISPs) have intrinsic incentives to cooperate with other network operators in order to expand access for each network. Transit and peering agreements are one such form of cooperation: Operators expand network connectivity by agreeing to carry each other's traffic under accepted conditions.[12] These agreements create benefits and responsibilities for both parties as each enjoys increased connectivity while shouldering increased monitoring for abusive activities. To be a successful network on the Internet, then, is to carefully monitor traffic for illegal and destructive online activity or risk losing connectivity through lost peering or transit agreements.[13]

The threat of rescinding these agreements, or "depeering," is a powerful mechanism in promoting voluntary monitoring of Internet traffic. ISPs that tolerate cyber criminals or destructive activities in their traffic, sometimes called "bulletproof hosts," face an uphill battle. Although cyber criminals are often willing to pay considerable premiums for their services, bulletproof hosts rarely exist for very long because, once exposed, they are shunned by the rest of the Internet. This was the

9. Although some policymakers and commentators routinely reference growing cybersecurity risks and perceived breaches, there is evidence that much of this panic is overblown. See Adam Thierer, "Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle," *Minnesota Journal of Law, Science & Technology* 14, no. 1 (2013): 309–86, http://mercatus.org/sites/default/files/Technopanics-by-Adam-Thierer_MN-Journal-Law-Science-Tech-Issue-14-1.pdf.
10. Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: Massachusetts Institute of Technology, 2010), 160–61.
11. *Ibid*., 163.
12. Bill Woodcock and Vijay Adhikari, "Survey of Characteristics of Internet Carrier Interconnection Agreements," Packet Clearing House, May 2, 2011, http://www.pch.net/resources/papers/peering-survey/PCH-Peering-Survey-2011.pdf. This analysis suggests that 99.5 percent of the analyzed agreements are informal "handshake" agreements with no written contract.
13. Eli Dourado, "Internet Security without Law: How Service Providers Create Order Online" (Working Paper No. 12-19, Mercatus Center at George Mason University, Arlington, VA, June 2012), http://mercatus.org/sites/default/files/ISP_Dourado_WP1219.pdf. Emergent informal arrangements exist both on and offline. For an exposition of the history and mechanism of bottom-up rules evolving without legislation, see Robert Ellickson, *Order without Law: How Neighbors Settle Disputes* (Cambridge, MA: Harvard University Press, 1994).

case for McColo, a defunct web-hosting service provider that was notorious for allowing "some of the most disreputable cyber-criminal gangs in business today."[14] Once alerted to these transgressions, McColo's upstream providers quickly terminated their relationships with McColo to avoid being depeered themselves.[15] The same fate befell similar bulletproof hosts like the Russian Business Network (RBN),[16] Atrivo/Intercage,[17] Troyak,[18] and Proxiez.[19]

Dynamic cybersecurity provision is also proactive. Mueller writes,

> Interpersonal and organizational networks among Internet service providers, computer security incident response teams (CSIRTs or CERTs), domain name registrars, hosting companies, email-based expert discussion forums, the information technology departments of major user organizations and government agencies, and a burgeoning market for private security services bear the brunt of the burden of protecting networks.[20]

These groups employ technical experts to monitor traffic for destructive activities and warn parties of potential security threats. Researchers at organizations like Carnegie Mellon University's CERT Coordination Center analyze the reported cybersecurity incidents to develop and recommend threat mitigation and prevention strategies.[21] The nonprofit Packet Clearing House provides a secure communication platform for network administrators to instantly warn one another of suspicious network activity.[22] Many private ISPs invest in notification systems that alert customers when their computers become infected.[23] Best practices for mitigating harm

14. Brian Krebs, "Major Source of Online Scams and Spams Knocked Offline," *Washington Post*, November 11, 2008, http://voices.washingtonpost.com/securityfix/2008/11/major_source_of_online_scams_a.html.
15. Brian Krebs, "Host of Internet Spam Groups Is Cut Off," *Washington Post*, November 12, 2008, http://articles.washingtonpost.com/2008-11-12/news/36871006_1_spam-e-mails-junk-e-mail-ironport.
16. Brian Krebs, "Russian Business Network: Down, but Not Out," *Washington Post*, November 7, 2007, http://blog.washingtonpost.com/securityfix/2007/11/russian_business_network_down.html.
17. Brian Krebs, "Scammer-Heavy U.S. ISP Grows More Isolated," *Washington Post*, September 5, 2008, http://voices.washingtonpost.com/securityfix/2008/09/scam-heavy_us_isp_grows_more_i.html.
18. Robert McMillan, "After Takedown, Botnet-Linked ISP Troyak Resurfaces," *Computerworld*, March 10, 2010, http://www.computerworld.com/s/article/9169118/After_takedown_botnet_linked_ISP_Troyak_resurfaces.
19. Dan Goodin, "'Bulletproof' ISP for Crimeware Gangs Knocked Offline," *Register*, May 14, 2010, http://www.theregister.co.uk/2010/05/14/zeus_friendly_proxiez_mia/.
20. Mueller, *Networks and States*, 163.
21. Eli Dourado, "Internet Security without Law."
22. Packet Clearing House, "INOC-DBA," Packet Clearing House website, accessed January 14, 2014, http://www.pch.net/inoc-dba/.
23. Kelly Jackson Higgins, "ISP Backlash over Feds' Bot Notification Initiative," *Dark Reading* (October 5, 2011), http://www.darkreading.com/risk/isp-backlash-over-feds-bot-notification-initiative/d/d-id n1136432?.

from botnet activity are shared among multiple organizations, including the Internet Engineering Task Force, the not-for-profit open standards organization that designs core Internet protocols.[24] These and other dynamic cybersecurity solutions allow rapid cooperation and targeting of destructive online activity.[25]

THE CYBERSECURITY FRAMEWORK: TECHNOCRATIC CYBERSECURITY PROVISION

The Cybersecurity Framework attempts to use technocratic means to generate outcomes similar to those of dynamic cybersecurity provision. Executive Order 13636 calls on the attorney general, secretary of Homeland Security, and director of national intelligence to produce "unclassified reports of cyber threats to the U.S. homeland," disseminate these reports to the "critical infrastructure entities authorized to received them," and consult with "private sector, subject-matter experts" for advice on how best to reduce and mitigate these cyber risks.[26] As directed by Presidential Policy Directive 21 (PPD-21),[27] the Department of Homeland Security (DHS) finalized a listing of the critical sectors that fall into the category of "critical infrastructure entities" along with their "associated critical functions and value chains."[28] The department identifies 16 critical infrastructure sectors,[29] which are divided into smaller segments based on the "end product produced." Each sector is assigned a Sector-Specific Plan (SSP) that details "how the National Infrastructure Protection Plan risk management framework is implemented within the context of the unique characteristics and risk landscape of the sector."[30] A Sector-Specific Agency (SSA) is assigned to each sector to identify and

24. J. Livingood, N. Mody, and M. O'Reirdan, "Recommendations for the Remediation of Bots in ISP Networks," Request for Comments 6561, Internet Engineering Task Force website, March 2012, http://www.ietf.org/rfc/rfc6561.txt.
25. Software Engineering Institute, *2010 CERT Research Report*, Software Engineering Institute at Carnegie Mellon University, 2011, http://www.cert.org/research/2010research-report.pdf.
26. "Improving Critical Infrastructure Cybersecurity," Executive Order 13636, part III, 78 Fed. Reg. 33 (February 12, 2013), http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
27. "Critical Infrastructure Security and Resilience," Presidential Policy Directive 21, 78 Fed. Reg. 34 (February 12, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. HSPD-7 created the initial list of critical infrastructure sectors and directed the Department of Homeland Security to further identify, prioritize, and coordinate the protection of this vulnerable category. PPD-21 superseded this directive, but many of the SPPs for identified critical infrastructure were therefore drafted or released before PPD-21 was enacted.
28. Department of Homeland Security, "Critical Infrastructure Sectors," Homeland Security website, accessed January 1, 2014, http://www.dhs.gov/critical-infrastructure-sectors.
29. The current sectors listed are the Chemical Sector; Commercial Facilities Sector; Communications Sector; Critical Manufacturing Sector; Dams Sector; Defense Industrial Base Sector; Emergency Services Sector; Energy Sector; Financial Services Sector; Food and Agriculture Sector; Government Facilities Sector; Healthcare and Public Health Sector; Information Technology Sector; Nuclear Reactors, Materials, and Waste Sector; Transportation Systems Sector; and Water and Wastewater Systems Sector.
30. Department of Homeland Security, "Critical Infrastructure Sectors."

assist private organizations in implementing the relevant SSP. The Department of Energy is the SSA for the Energy Sector, for instance, and the Department of the Treasury is the SSA for the Financial Services Sector. Private stakeholders that fall into identified sector categories[31] will accordingly be encouraged to comply with the new Cybersecurity Framework.

The Cybersecurity Framework has three parts.[32] The first, the Framework Core, is a compilation of best cybersecurity practices for each category and level of each critical infrastructure sector, as determined by regulators and industry consultants. The framework does not explicitly detail how organizations will know whether or how they need to comply with the voluntary framework, but it is likely that the already existing Sector Coordinating Councils (SCCs) will promote and educate members on adoption once the framework takes effect. The framework text does note, however, that because "each organization's risk is unique . . . the tools and methods used to achieve the outcomes described by the Framework will vary."[33] The Framework Core standards are divided into five broad functions—identify, protect, detect, respond, and recover—which are then divided into categories and subcategories.

The second part of the framework consists of the Framework Implementation Tiers, which are measures of compliance with each function, category, and subcategory. The tiers range from Partial (Tier 1) to Adaptive (Tier 4). The third part of the framework is the Framework Profile, an organization's unique "score" of compliance with the recommended level of cybersecurity.

The Cybersecurity Framework is merely the latest iteration of federal aspirations to intervene in the dynamic provision of cybersecurity. This voluntary

---

31. However, it is possible that critical infrastructure assets that do not meet the critical infrastructure criteria may still be included in the category if the DHS determines that the infrastructure has received a "specific, credible threat." See Government Accountability Office, *Critical Infrastructure Protection: DHS List of Priority Assets Needs to Be Validated and Reported to Congress*, GAO-13-296 Report to Congressional Requesters, March 2013, http://www.gao.gov/assets/660/653300.pdf. Another report from the Internet Policy Task Force of the Department of Commerce urges policymakers to consider businesses and industries that fall outside the already broad definition of "critical infrastructure." Called the "Internet and Information Innovation Sector" (I3S), this new classification would include organizations that provide functions and services relating to "provision of information services and content, facilitation of Internet transactional services, storage and hosting of publicly accessible content, and application, browser, social network, and search providers." See Internet Policy Task Force, "Cybersecurity, Innovation and the Internet Economy," Department of Commerce Green Paper, June 2011, http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_Final Version.pdf. The recent "Heartbleed" vulnerability in the OpenSSL cryptographic software library, which allowed external parties to access private memory in systems that used OpenSSL, has prompted some security commentators to push for an even broader definition of critical infrastructure to include similar software. See Dan Kaminsky, "Be Still My Breaking Heart," *Dan Kaminsky's Blog*, April 10, 2014, http://dan kaminsky.com/2014/04/10/heartbleed/. The technocratic approach would be similarly ill-equipped to provide adequate incentives for these broader conceptions of "critical infrastructure."

32. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-frame work-021214.pdf.

33. Ibid., 3.

program comes on the heels of stalled legislative attempts to enact compulsory cybersecurity standards, such as the Cyber Intelligence Sharing and Protection Act[34] and the Cybersecurity Act.[35] Many cybersecurity lobbyists suggest that the voluntary Cybersecurity Framework does not go far enough, and these lobbyists have called on the Obama administration to impose a compulsory cybersecurity standard.[36] Framework developers have already suggested a schedule of government benefits to incentivize program participation.[37] These incentives could be strong enough to put nonadopters at a competitive disadvantage. Similarly, federal initiatives have sometimes been "voluntary in name only."[38] Whether voluntary, pseudo-voluntary, or compulsory, technocratic cybersecurity standards threaten to undermine dynamism in cybersecurity and Internet governance while opening the door for rent-seeking and corruption.

DYNAMIC CYBERSECURITY FOR CRITICAL PHYSICAL INFRASTRUCTURE

What about cyber threats to critical physical infrastructure? While dynamic standards have emerged to provide flexible and adequate general network cybersecurity, many worry that the unique cybersecurity for the physical infrastructure, like power grids and transit systems, are lacking.[39] This infrastructure's unprecedented exposure to potential cyber vulnerabilities leads some to conclude that a centrally driven, public-private standard for information sharing and coordination is the only viable solution.

Data breaches and losses present similar challenges to businesses. As more personal and professional information moves online, data breaches and losses become

34. Cyber Intelligence Sharing and Protection Act of 2013, H.R. 624, 113th Congress (2013), http://thomas.loc.gov/cgi-bin/bdquery/z?d113:h.r.624:.

35. Cybersecurity Act of 2012, S. 2105, 112th Congress (2012), http://thomas.loc.gov/cgi-bin/bdquery/z?d112:s.2105:.

36. Michael S. Schmidt and Nicole Perlroth, "Obama Order Gives Firms Cyberthreat Information," *New York Times*, February 12, 2013, http://www.nytimes.com/2013/02/13/us/executive-order-on-cyber security-is-issued.html?_r=0.

37. Some incentives proposed so far include targeted grants, process preference, expedited government service delivery, rate recovery for public utilities, and liability limitation for firms that adopt the framework. See Michael Daniel, "Incentives to Support Adoption of the Cybersecurity Framework," *White House Blog*, August 6, 2013, http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.

38. Jerry Brito, "An Offer You Can't Refuse: 'Agency Threats' and the Rule of Law," *Harvard Journal of Law and Public Policy* 37 (forthcoming 2014).

39. Somewhat confusingly, several popular calls for a government-driven integration of critical infrastructure cybersecurity have only provided examples of breaches to basic network security to bolster their cases. *Cyber War*, for example, sounds the alarm about hypothetical destructive threats to critical infrastructure, but only provides examples of "primitive" DDoS attacks that are already adequately handled by the dynamic cybersecurity provision detailed in the second section. See Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: Ecco, 2012).

more possible. Many businesses and public organizations have yet to update their information technology and cybersecurity practices in the face of this wave of digitalization, and the procrastination is hurting. According to a report from the Online Trust Alliance, a nonprofit industry research and education organization, 2013 was the worst year on record for data breaches.[40] Consistent with previous research,[41] an estimated 89 percent of these breaches could have been prevented through basic routine security practices.[42] These breaches create huge costs for customers and companies alike.

Government agencies like the DHS, Department of Commerce, and National Institute of Standards and Technology have recently looked to cybersecurity insurance as a market-driven solution for critical infrastructure and information cybersecurity vulnerabilities.[43] In fact, the Obama administration expressed hope that the Cybersecurity Framework would help insurance companies standardize cyber risk assessments enough to allow cybersecurity premiums to become affordable.[44] Private industry has also shown interest in cybersecurity insurance.[45] While many reformers see the development of a robust cybersecurity insurance market as merely one prong of their broader effort, the cybersecurity insurance initiative alone could sufficiently address concerns.

The cybersecurity insurance industry is small, but growing;[46] it faces early challenges to development. Businesses can currently purchase insurance products from private companies to hedge Internet and information technology risks that are not covered in other insurance packages, but these packages are limited and often inconsistent.[47] Cybersecurity insurance packages can include first-party

40. Online Trust Alliance, "2014: Data Protection and Breach Readiness Guide," last updated April 7, 2014, https://otalliance.org/resources/incident/2014OTADataBreachGuide.pdf.
41. Verizon Risk Team, "2012 Data Breach Investigations Report," Verizon website, 2012, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf.
42. Online Trust Alliance, "2014: Data Protection and Breach Readiness Guide."
43. Department of Homeland Security, "Cybersecurity Insurance Workshop Readout Report," November 2012, http://www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf; Internet Policy Task Force, "Cybersecurity, Innovation and the Internet Economy," Department of Commerce Green Paper, June 2011, http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_Final Version.pdf.
44. Michael Daniel, "Incentives to Support Adoption of the Cybersecurity Framework," *White House Blog*, August 6, 2013, http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.
45. Andrew Braunberg, "Multiple Drivers for Cyber Security Insurance: Expectations Placed on Insurance Carriers Rise with Market Growth," NSS Labs Analyst Brief, NSS Labs website, November 14, 2013, https://www.nsslabs.com/reports/multiple-drivers-cyber-security-insurance.
46. A 2013 research report from Experian, an information services and credit report company, reports that 31 percent of companies currently had cybersecurity insurance policies while another 39 percent had plans to purchase coverage in the future. See Christopher M. Matthews, "Cybersecurity Insurance Picks Up Steam, Study Finds," *Wall Street Journal*, August 7, 2013, http://blogs.wsj.com/riskandcompliance/2013/08/07/cybersecurity-insurance-picks-up-steam-study-finds/.
47. Ibid.

coverage of losses due to hacking, distributed denial-of-service (DDoS) attacks, and data destruction, as well as providing liability coverage and security audits.[48]

Cybersecurity insurance is an attractive solution to the problem of critical infrastructure protection for several reasons. First, it can provide competitive and flexible coverage that is tailored directly to the unique needs of each industry and organization.[49] Such coverage would reduce the uncertainty about cyber threats that businesses currently face and provide them with financial and strategic recovery in the event of a breach. Second, firms would face strong incentives to continually invest in and improve their internal system security so that their premiums would remain manageable.[50] Insurance companies would encourage clients with substandard security practices to improve through audits and rate pressure. As a spillover effect, insurance companies would learn best practices from experiences with other clients and could continually improve the net level of cybersecurity by developing better recommendations and standards in the future.[51] Finally, a cybersecurity insurance solution would more fairly and accurately price and distribute risk and liability through the use of a price mechanism.[52] Unlike regulators and even public-private partnerships, private insurance analysts would be guided by competition and the profit motive to apply the best possible risk assessments in order to provide the maximum amount of coverage for their clients at the lowest possible premiums.

Despite the attractiveness of a cybersecurity insurance solution, the market has struggled to adequately expand. Some brokers report that they have yet to sell a single cybersecurity insurance package after offering them for about a decade.[53] Information asymmetries and unclear risk pricing can explain the slow development of a robust cybersecurity insurance market.[54] Insurance analysts are unsure

48. Larry Clinton, "Cyber-Insurance Metrics and Impact on Cyber-Security," Internet Security Alliance White Paper, accessed January 14, 2014, http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf.
49. Ibid.
50. Jay P. Kesan, Ruperto P. Majuca, and William J. Yurcik, "The Economic Case for Cyberinsurance" (Illinois Law and Economics Working Papers Series No. LE04-004, 2004).
51. Ibid.
52. Jeffrey Kehne, "Encouraging Safety through Insurance Based Incentives: Financial Responsibility for Hazardous Wastes," *Yale Law Journal* 96, no. 2 (1986): 403–27.
53. Sarb Sembhi, "An Introduction to Cyber Liability Insurance Coverage," *Computer Weekly*, July 2013, http://www.computerweekly.com/news/2240202703/An-introduction-to-cyber-liability-insurance-cover.
54. Nikhil Shetty et al., "Competitive Cyber-Insurance and Internet Security," in *The Economics of Information Security and Privacy*, ed. Tyler Moore, David Pym, and Christos Ioannidis (New York: Springer, 2010), 229–47. Note that the model employed in this paper assumes a homogeneity of firms and information asymmetries for analytic purposes. This assumption, which the authors state is too simplistic for broad explanatory power but useful for their analysis, results in cybersecurity insurance that does not require security investment and improvement. For an explanation of how cybersecurity insurance can improve security, see Jay P. Kesan, Ruperto P. Majuca, and William J. Yurcik, "The Economic Case for Cyberinsurance" (Illinois Law and Economics Working Papers Series No. LE04-004, 2004).

exactly how to price risk in this new domain because they lack comparable precedents. Premiums for existing cybersecurity packages therefore tend to be cost-prohibitive for most companies, explaining the low adoption rate in the face of widespread industry interest. This creates a catch-22 of sorts: as long as premiums are prohibitively expensive, most companies will not be able to purchase them. But if no companies purchase insurance packages, then insurance companies cannot gather data and experience in cybersecurity risk assessment to more accurately price liabilities and lower premiums. A first mover with deep pockets and a strong desire for cybersecurity insurance is needed to break this disequilibrium.

One obvious candidate is the federal government. The federal government has already committed itself to improving its internal cybersecurity practices as part of the critical infrastructure protection program. Federal agencies could stimulate the development of a cybersecurity insurance market through a competitive bidding process for beneficial insurance coverage and reasonable premiums from private insurers. This would kick-start the heretofore illusory critical risk analysis process and enable insurers to derive needed information and develop best practices from their first big customer. Publicly chartered utilities and other protected industries and firms could, as a condition of their agreements with the relevant government body, be subsequently required to purchase cybersecurity insurance after the market has developed. Private firms that desire to purchase cybersecurity insurance would then be able to do so on their own. Firms that do not immediately purchase cybersecurity insurance would be at a competitive disadvantage and would therefore face strong incentives to purchase coverage.

Not only could this solution lower premiums and remedy information asymmetries, but the federal government would be leading by example and promoting adequate cybersecurity provision through market-driven means. SSAs' first-mover advantage would place them in a position to influence coverage levels and encourage proactive measures and auditing procedures from the start. Government officials and industry experts would still be collaborating and working to increase cybersecurity preparedness, but in this scenario incentives are more properly aligned and knowledge is more properly applied. The federal government would harness its comparative advantages of monopsonistic purchasing power and collaborative vision while tapping into the flexibility, experience, and innovation of profit-seeking cybersecurity and insurance companies. As mentioned above, the White House, Department of Homeland Security, and Department of Commerce already recognize the benefits of a thriving cybersecurity insurance market. However, the history of dynamic cybersecurity standards and practices suggests that the federal government itself need not develop standards for the insurance industry for standards to emerge.

PROBLEMS WITH THE CYBERSECURITY FRAMEWORK

The Cybersecurity Framework attempts to promote the outcomes of dynamic cybersecurity provision without the critical incentives, experimentation, and processes that undergird dynamism. The framework would replace this creative process with one rigid incentive toward compliance with recommended federal standards. The Cybersecurity Framework primarily seeks to establish defined roles through the Framework Profiles and assign them to specific groups. This is the wrong approach. Security threats are constantly changing and can never be holistically accounted for through even the most sophisticated flowcharts.[55] What's more, an assessment of DHS critical infrastructure categorizations by the Government Accountability Office (GAO) finds that the DHS itself has failed to adequately communicate its internal categories with other government bodies.[56] Adding to the confusion is the proliferating amalgam of committees, agencies, and councils that are necessarily invited to the table as the number of "critical" infrastructures increases.[57] By blindly beating the drums of cyber war and allowing unfocused anxieties to clumsily force a rigid structure onto a complex system, policymakers lose sight of the "far broader range of potentially dangerous occurrences involving cyber-means and targets, including failure due to human error, technical problems, and market failure apart from malicious attacks."[58] When most infrastructures are considered "critical," then none of them really are.[59]

This public-private partnership runs a high risk of becoming further mired in unwieldy top-down complexity.[60] Defining roles and responsibilities in this rigid way would leave US networks wide open to unanticipated vulnerabilities that develop in the future. Firms' former incentives to collaborate and innovate in response to changing security needs would be replaced with the simple incentive to increase their Framework Profile "score." In other words, the Cybersecurity Framework's metrics—no matter how carefully designed and updated—will incentivize firms to increase what is measured at the expense of what is not measurable.

---

55. Eli Dourado, "Internet Security without Law."
56. Government Accountability Office, *Critical Infrastructure Protection*.
57. Elizabeth Newell Jochum, "Critical Alliance," *Government Executive,* Government Executive website, October 1, 2009, http://www.govexec.com/magazine/magazine-news-and-analysis/2009/10/critical-alliance/30043/.
58. Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: U.S. Efforts to Secure the Information Age* (New York: Routledge, 2007).
59. Joel Schectman, "U.S. Gives Companies Cybersecurity Guidelines to Protect Critical Infrastructure," *Wall Street Journal*, October 23, 2013, http://blogs.wsj.com/cio/2013/10/23/u-s-gives-companies-cybersecurity-guidelines-to-protect-critical-infrastructure/.
60. Jena Baker McNeill and Richard Weitz, "How to Fix Homeland Security Critical-Infrastructure Protection Plans: A Guide for Congress," Heritage Foundation Backgrounder #2404, Heritage Foundation website, April 27, 2010, http://www.heritage.org/research/reports/2010/04/how-to-fix-homeland-security-critical-infrastructure-protection-plans-a-guide-for-congress.

This problem plagues incentive contracts with much simpler objectives.[61] The fuzzy, interdependent nature of "critical infrastructure cybersecurity" makes it that much more impervious to this kind of multivariate optimization. The federal government should first identify and understand the incentives and barriers that respectively generate benefits and problems in the current system before attempting to synthetically emulate and optimize the interdependent "parts" that planners currently prioritize. An improved cybersecurity system would not focus on assigning roles, as the Cybersecurity Framework does, but would explore ways to make our current dynamic cybersecurity provision even more responsive. Officials could meet with industry stakeholders, not to design a cybersecurity system from scratch, but to discover existing sources of friction that can be alleviated through government action, such as the declassification of security threats. In this way, the government could best improve cybersecurity by making minor tweaks on the margins of our existing, and largely adequate, cybersecurity provision.

It is worth noting that the federal government's track record of maintaining adequate cybersecurity provision and response for its own agency systems has been quite embarrassing. In 2012, at least 13 separate government bodies suffered major system breaches.[62] One employee of the Commodity Futures Trading Commission was fooled by a simple phishing email and unwittingly allowed hackers to steal the personal data and Social Security numbers of over 700 employees.[63] Dubbed a "failure of cybersecurity 101," a data breach of the Environmental Protection Agency Superfund servers left over 8,000 financial records and home addresses exposed.[64] Even the DHS, a key player in the new Cybersecurity Framework, has been vulnerable to cybersecurity breaches.[65] An internal report on DHS cybersecurity more explicitly reveals its deficiencies.[66] In addition to lackluster "personal identity verification compliant logical access" systems and "incident detection and analysis" capabilities, the report warns that its "systems are being operated without authority to operate; plans of action and milestones are not being created for all known

61. George P. Baker, "Incentive Contracts and Performance Measurement," *Journal of Political Economy* 100, no. 3 (1992): 598–614.

62. Paul Rosenzweig, "The Alarming Trend of Cybersecurity Breaches and Failures in the U.S. Government Continues," Issue Brief #3772, Heritage Foundation website, November 13, 2012, http://www.heritage.org/research/reports/2012/11/cybersecurity-breaches-and-failures-in-the-us-government-continue.

63. Silla Brush, "CFTC Data Breach Risks Employees' Social Security Numbers," *Bloomberg Business Week*, Bloomberg website, June 25, 2012, http://www.businessweek.com/news/2012-06-25/cftc-data-breach-risks-employees-social-security-numbers.

64. Amber Corrin, "Was the EPA Data Breach a Failure of Cybersecurity 101?," *FCW*, August 3, 2012, http://fcw.com/articles/2012/08/03/epa-security-breach-contractors-virus.aspx.

65. Adam Jones, "Another US Government Site Hacked!," *Security Magazine*, June 23, 2012, http://www.seczine.com/article/hacking-news/230612/another-us-gov-site-hacked.php.

66. Department of Homeland Security Office of the Inspector General, *Evaluation of DHS' Informational Security Program for Fiscal Year 2013*, *OIG-14-09*, November 2013, http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-09_Nov13.pdf.

information security weaknesses or mitigated in a timely manner; and baseline security configuration settings are not being implemented for all systems."[67] Before the DHS offers its services to private operators of critical infrastructure, it should get its own house in order.

This lack of cybersecurity is a systemic problem. A recent GAO study of eight federal agencies' procedures for responding to data breaches finds that agency policies, even when developed, are inconsistently implemented.[68] More alarming is the finding that the federal government's internal procedures for reporting and following up on identified and analyzed cyber breaches are rarely followed and have "provided few benefits."[69] The GAO report cites data from the US Computer Emergency Readiness Team (US-CERT) that the number of cybersecurity breaches involving personally identifiable information among US federal agencies has dramatically increased from around 10,000 incidents in 2009 to more than 22,000 incidents in 2012. This is not the first time that the federal government has failed to meet the standards it set for itself. Before this most recent report, the GAO prepared four separate audits of federal cybersecurity practices from 2007 to 2009.[70] Each report identified vulnerabilities in agencies' existing systems and noted failures to comply with internal procedures and agency directives. The Office of Management and Budget (OMB) sometimes responded to these reports by outlining new plans to address vulnerabilities, but the most recent GAO report notes that these fixes often fail to materialize.[71] If the federal government cannot manage to get its own agencies and employees to comply with their own internal procedures, it is hard to see how they can coordinate the cybersecurity policy of large portions of the nation's critical infrastructure.

Some of the justifications for the Cybersecurity Framework that its supporters use underscore a weakness of their proposed policies. As noted earlier, many of the hypothetical cyber doom scenarios that cybersecurity hawks present are unsubstantiated. One reason that they resort to using imagined scenarios is the

---

67. Ibid.

68. Government Accountability Office, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent*, GAO-14-34 Report to Congressional Requesters, December 2013, http://www.gao.gov/assets/660/659572.pdf.

69. Ibid.

70. Government Accountability Office, *Privacy: Lessons Learned about Data Breach Notification*, GAO-07-657, April 30, 2007, http://www.gao.gov/products/GAO-07-657; Government Accountability Office, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737, June 4, 2007, http://www.gao.gov/products/GAO-07-737; Government Accountability Office, *Information Security: Protecting Personally Identifiable Information*, GAO-08-343, January 25, 2008, http://www.gao.gov/products/GAO-08-343; Government Accountability Office, *Identity Theft: Governments Have Acted to Protect Personally Identifiable Information, but Vulnerabilities Remain*, GAO-09-759T, June 17, 2009, http://www.gao.gov/products/GAO-09-759T.

71. Government Accountability Office, *Information Security: Agency Responses to Breaches of Personally Identifiable Information.*

government overclassification of cybersecurity threats and activity.[72] Setting aside the dulling effect this has on advocates' rhetoric, this admission of federal secret-keeping regarding cybersecurity threats presents a catch-22 scenario. If this information is so critical to cybersecurity provision that it warrants federal classification, businesses and organizations that lack access are put at risk by their ignorance. It is impossible to know the extent of cybersecurity risks if critical information is kept secret by the government. Some prominent voices within the cybersecurity community agree that cybersecurity information is overclassified to the point of being counterproductive. Michael Hayden, former director of both the National Security Agency and the Central Intelligence Agency, declares, "Let me be clear: This stuff is overprotected. It is far easier to learn about physical threats from US government agencies than to learn about cyber threats. . . . If we want to shift the popular culture, we need a broader flow of information to corporations and individuals to educate them on the threat. To do that we need to recalibrate what is truly secret."[73] Proponents of the Cybersecurity Framework talk a lot about "information sharing," but in practice, the federal government has restricted cybersecurity information-sharing to the alarm of even the cyber alarmists. So long as the federal government continues this practice of overclassifying relevant cybersecurity information, the Cybersecurity Framework will be a hollow promise.

There are additional unclear implications of the Cybersecurity Framework that could also hurt innovation. Much of the Internet's success has been predicated on its culture of permissionless experimentation. This productive ethos was acknowledged and protected by proactive policymakers in section 230 of the Communications Decency Act of 1996, which stipulates that organizations cannot be held legally liable for digital content traversing their networks or posted to their websites by users.[74] If the Cybersecurity Framework is given legislative teeth and compulsory backing in the future, ISPs could be legally and financially liable for online activity deemed to be in breach of the framework. The considerable cost of these new liabilities could have chilling effects on innovation in cyberspace.

Finally, the Cybersecurity Framework opens the door to rent-seeking and corruption. The parties identified to develop and implement the Cybersecurity Framework harbor clear conflicts of interest. Regulators eager to exert control over Internet governance, and cybersecurity industry insiders seeking their first pick of government contracts, will both be placed in positions of power to direct the development

72. Jerry Brito and Tate Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy," *Harvard National Security Journal* 3 (2011): 39–84, http://harvardnsj.org/wp-content/uploads/2012/01/Vol.-3_Brito_Watkins.pdf.

73. Michael V. Hayden, "The Future of Things 'Cyber,'" *Strategic Studies Quarterly* 3, no. 5 (2011): 3–7, http://www.au.af.mil/au/ssq/2011/spring/hayden.pdf.

74. Protection from copyright infringement, however, is not granted through section 230. See *Communications Decency Act of 1996*, http://transition.fcc.gov/Reports/tcom1996.txt.

of national cybersecurity provision. Some of these same actors have been vociferous in hyping the specter of cyber war and in calling for even stronger state-imposed Internet controls.[75] Like the military-industrial complex that exaggerates foreign threats for profit, initiatives like the Cybersecurity Framework will add avenues through which corporations can extract public wealth for private gain.[76]

Even a pared-down federal cybersecurity initiative could create perverse incentives. For instance, the proposed federally created or influenced private cybersecurity insurance market could be "free market" in name but driven by clientelism and corruption in practice. The benefits of federally driving the creation of a private cybersecurity insurance market should be considered alongside the potential costs of cronyism and path dependence. While the potential for corruption in any government intervention is unavoidable, compared to the likeliest alternatives, the cybersecurity insurance market option may the one that best minimizes corrupting influences while maximizing desired outcomes of cybersecurity provision, improvement, and preparedness. The broad and complex Cybersecurity Framework allows even more channels for perverse self-interest at public expense. By politically strengthening entrenched interests in the cybersecurity industry, we run the risk of ultimately weakening cybersecurity.

CONCLUSION

The Cybersecurity Framework creates more problems than it solves. A lack of a single technocratic standard does not imply a lack of any standard. The imagined specter of cyber doom does not a national security crisis make. As a dynamic system, the incentives and norms that guide Internet activity spontaneously generate low-cost, effective solutions to shared problems.

To improve cybersecurity provision for critical infrastructure, the federal government should take a different approach. We recommend

- narrowly defining the term "critical infrastructure" to increase clarity and focus priorities,
- cultivating the development of a private cyber insurance market by purchasing coverage for breach-riddled federal agencies, and
- removing barriers to the dynamic development of cybersecurity provision for critical infrastructures by declassifying information about known cyber threats.

These steps will help to improve cybersecurity protection for critical infrastructure and general systems alike. By encouraging emergent solutions, the federal

75. Brito and Watkins, "Loving the Cyber Bomb?"
76. Ibid.

government could help improve the dynamic fabric of our cybersecurity ecosystem. The Cybersecurity Framework threatens to undermine this largely functioning system by imposing a brittle, technocratic standard that benefits specific interests and diminishes the incentives for cybersecurity innovation.