

# Texas Law Review

## *See Also*

Response

### Cybersecurity: Toward a Meaningful Policy Framework

Peter M. Shane\*

Karson K. Thompson's note, *Not Like an Egyptian: Cybersecurity and the Internet Kill Switch Debate*,<sup>1</sup> is a useful contribution to discussions within—and, one hopes, beyond—academic circles about a set of issues both hugely important and little understood. Its inventory of pending proposals<sup>2</sup> and its caution against undue alarmism<sup>3</sup> are both especially welcome. Protecting networks, computers, programs, and data—and the critical infrastructures on which they rely—from attack, damage, or unauthorized access<sup>4</sup> could hardly be more important given contemporary society's

---

\* Jacob E. Davis and Jacob E. Davis II Chair in Law, Moritz College of Law, The Ohio State University. Along with my friend and former colleague, Dr. Jeffrey Hunker, I had the privilege last spring of organizing a symposium at Ohio State on cybersecurity policy, under the sponsorship of *I/S: A Journal of Law and Policy for the Information Society*. The unpublished papers cited in footnotes below were presented at that symposium and will be published next spring in Volume 8, Issue 2 of *I/S*. Carolina Academic Press is also publishing versions of the papers as chapters of PETER M. SHANE & JEFFREY HUNKER, *CYBERSECURITY: SHARED RISKS, SHARED RESPONSIBILITIES* (forthcoming 2012). I am deeply indebted to both Dr. Hunker and the other symposium participants for such understanding as I have of the world of cyber policy. Errors of fact and judgment, of course, remain solely my responsibility.

1. Karson K. Thompson, Note, *Not Like an Egyptian: Cybersecurity and the Internet Kill Switch Debate*, 90 TEXAS L. REV. 465 (2011).

2. See generally *id.* at 482–88 (outlining seven cybersecurity bills before the 112th Congress).

3. See *id.* at 470 (“In some situations, the alarmist rhetoric has lost touch with reality . . . . Though such wild speculation is demonstrably false, it nevertheless serves to create an atmosphere of danger and fear in an attempt to justify government restrictions.” (footnotes omitted)).

4. This definition of cybersecurity is based on *Cybersecurity*, WHATIS.COM, <http://whatis.techtarget.com/definition/cybersecurity.html> (last updated Dec. 17, 2010), which has been cited approvingly by the Securities and Exchange Commission in its guidance on corporate

ubiquitous dependence on digital information and communication technologies. We need talented, cyber-literate lawyers to focus on these issues.

Following both his introductory account of the Internet's development, which helps to explain its vulnerabilities,<sup>5</sup> and his survey of America's current cyber policy and regulatory landscape,<sup>6</sup> Mr. Thompson offers a six-point "framework" to serve as what he calls "a jumping-off point for a unified and comprehensive approach to national cybersecurity."<sup>7</sup> These points<sup>8</sup> include:

1. streamlining the federal government's cybersecurity policy apparatus under what I infer to be a single presidential appointee subject to the Senate's advice and consent;<sup>9</sup>
2. modifying the Communications Act of 1934 to make certain the absence of any presidential "kill switch" authority;<sup>10</sup>
3. standardizing federal computer networks to permit the verification, tracking, and control of access under a standard security scheme;<sup>11</sup>
4. using federal purchasing power to incentivize the development of more security-protective hardware and software in the open market;<sup>12</sup>
5. imposing "smart regulation" to govern security practices by utility networks and tier-one internet service providers (ISPs) that would (1) isolate utility networks from the open-to-everyone Internet and (2) permit or require the ISPs "to detect and cut off malicious traffic";<sup>13</sup> and
6. ramping up federal investment in education, job training, recruitment, and scientific research.<sup>14</sup>

---

disclosures relative to cybersecurity. DIV. OF CORPORATE FIN., SEC. & EXCH. COMM'N, CF DISCLOSURE GUIDANCE: TOPIC NO. 2, CYBERSECURITY (Oct. 13, 2011), *available at* <http://www.sec.gov/divisions/corpin/guidance/cfguidance-topic2.htm>. My version incorporates network-dependent infrastructure among the subjects of protection.

5. *See* Thompson, *supra* note 1, at 466–70 (chronicling the Internet's development and the emergence of security threats, including viruses).

6. *See generally id.* at 478–88 (outlining current emergency powers, presidential policies, and congressional proposals concerning cybersecurity).

7. *See generally id.* at 489–95 (setting forth the framework for national cybersecurity).

8. For ease, subsequent references to these proposals are in the form of "Point X."

9. Thompson, *supra* note 1, at 491.

10. *Id.* at 491–92.

11. *Id.* at 492.

12. *Id.* at 492–93.

13. *Id.* at 493–94.

14. *Id.* at 495. Point 6 also includes the development of a capacity within the federal government to find vulnerabilities in private networks and report them to owners. *Id.* The specter of government hacking into private networks strikes me as raising profound Fourth Amendment problems.

But for all that is useful in Mr. Thompson's note, these points do not really add up to the policy framework that the United States needs. Elements of Points 1 and 3 are likely both unwise and impracticable, and Point 5 is both partly self-contradictory and too modest. (I do not quarrel with Point 2 because, among other reasons, an Egypt-style Internet blackout is probably not feasible in the United States. As to Point 4 and most of Point 6, one can respond only, "Absolutely!") Nor are these points connected in any obvious way to a set of principles that really cohere as a "framework." In this brief Response, I will try to explain these specific points but, perhaps more important, will illuminate the nature of the difficulties facing the current cyber-policy enterprise in a way that suggests the rather larger questions that need to be tackled.

At the outset, while I applaud Mr. Thompson's antialarmist tone, I would like to suggest that his analysis really does not quite capture the seriousness of the current moment. Yes, there is no real likelihood that some evildoer currently possesses the capacity to bring down the United States's banks, transportation systems, electric grid, and communication systems through catastrophic cyber aggression. But cyber war is a reality.<sup>15</sup> Cybercrime is advancing in both volume and sophistication.<sup>16</sup> And cyberexploitation—hacking that aims to accomplish information theft from both government<sup>17</sup> and sensitive private sources<sup>18</sup>—is clearly a growth industry. While it is easy to exaggerate the real threat of cyber aggression intending to disrupt critical United States systems, this is due in part to the realization by both criminal syndicates and other nations that they have more to gain from forms of aggression that achieve access to sensitive data while leaving primary-network functions intact.<sup>19</sup> On a day-to-day basis, it is better strategy to steal than disrupt.

---

15. See Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, GUARDIAN, May 17, 2007, available at <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia> (recounting Russia's disabling of websites of Estonian government ministries, political parties, banks, and others).

16. For a discussion of incentives to engage in cyber attacks in the context of recent attacks, see JEFFREY HUNKER, CREEPING FAILURE: HOW WE BROKE THE INTERNET AND WHAT WE CAN DO TO FIX IT 38–43 (2010).

17. See, e.g., Thom Shanker & Elisabeth Bumiller, *Hackers Gained Access to Sensitive Military Files*, N.Y. TIMES, July 15, 2011, available at <http://www.nytimes.com/2011/07/15/world/15cyber.html> (describing a hacking attack from a foreign intelligence service, which stole thousands of Pentagon files from a military contractor).

18. See, e.g., Joe McDonald, *Security Firm: Hackers Hit Chemical Companies*, SALON.COM (Nov. 1, 2011), [http://news.salon.com/2011/11/01/security\\_firm\\_hackers\\_hit\\_chemical\\_companies](http://news.salon.com/2011/11/01/security_firm_hackers_hit_chemical_companies) (reporting a security company's discovery of forty-eight Chinese cyber attacks on chemical- and military-related companies in 2011).

19. See HUNKER, *supra* note 16, at 51 (identifying (1) the incentives for criminal syndicates and governments to engage in this activity, and (2) their efforts to infiltrate, rather than destroy, data systems).

What makes all of this yet more anxiety provoking, however, is not just technical complexity but policy failure. And by “policy failure,” I mean both existing policy that is inadequate and policy we need to exist that does not. Consider the opening paragraphs of a recent news story:

Just before the American-led strikes against Libya in March, the Obama administration intensely debated whether to open the mission with a new kind of warfare: a cyberoffensive to disrupt and even disable the Qaddafi government’s air-defense system, which threatened allied warplanes.

While the exact techniques under consideration remain classified, the goal would have been to break through the firewalls of the Libyan government’s computer networks to sever military communications links and prevent the early-warning radars from gathering information and relaying it to missile batteries aiming at NATO warplanes.

But administration officials and even some military officers balked, fearing that it might set a precedent for other nations, in particular Russia or China, to carry out such offensives of their own, and questioning whether the attack could be mounted on such short notice. *They were also unable to resolve whether the president had the power to proceed with such an attack without informing Congress.*<sup>20</sup>

We may contrast the legal problems identified in this story with the ambiguity that troubles Mr. Thompson as to whether the Communications Act of 1934 could plausibly be read to authorize a presidential shutdown of Internet traffic—that is, a kill switch.<sup>21</sup> It seems doubtful, for at least two reasons, that the kill switch question will ever actually ripen into operational significance. First, the sheer number of ISPs and backbones in the United States together with the all-but-innumerable connections between United States networks and the rest of the world make a workable kill switch unlikely.<sup>22</sup> Second, the unintended social, economic, and even security impacts of any attempted United States Internet shutdown could be disastrous<sup>23</sup>—as the White House would no doubt anticipate. In other words, even if a kill switch existed, no one would likely ever throw it. Not having policy, however, as to the proper analysis of cyber aggression under the

---

20. Eric Schmitt & Thom Shanker, *U.S. Debated Cyberwarfare in Attack Plan on Libya*, N.Y. TIMES, Oct. 18, 2011 (emphasis added), available at <http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html> (emphasis added).

21. See Thompson, *supra* note 1, at 478–79, 491 (setting forth the broad scope of presidential powers in this area, and arguing for a modification of the Communications Act of 1934 to limit those powers).

22. I am grateful to Dr. Jeffrey Hunker for pointing this out to me.

23. Gregory T. Nojeim, *Cybersecurity: Ideas Whose Time Has Not Come—And Shouldn’t*, 8 I/S: J.L. & POL’Y FOR INFO. SOC’Y (forthcoming 2012).

international law of armed conflict<sup>24</sup>—and not knowing the scope of the President’s authority to use cyber techniques offensively against a military adversary<sup>25</sup>—these are policy lacunae of immediate and undoubted significance. We do not have to speculate as to whether policy uncertainty in these respects is operationally significant; Libya already establishes the point.

As I see it, there are four primary reasons for the cyber-policy mess that exists. One, to be sure, is the “bewildering array of overlapping responsibilities” scattered among government offices and departments, which is “ripe for bureaucratic territoriality and confusion.”<sup>26</sup> A second is the inescapable fact that government responsibility for cybersecurity must be shared among military and civilian authorities, thus involving institutions both inherently competitive and endowed with significantly different organizational cultures (and considerable heterogeneity on each side of that dividing line) regarding both information sharing and decision-making process.<sup>27</sup> A third is that without question, most of the networks (and the dependent critical infrastructures) that need protecting are in private hands, and issues of public–private relations are currently awash in shibboleths about the wonders of free markets and the dangers of regulation that have seemingly disabled serious talk about the kinds of regulation that we need.<sup>28</sup> Finally, and perhaps most critical of all, there is no reason to believe that the public—or, for that matter, Congress—has any significant understanding of cybersecurity as an actual problem of policy. The pursuit of cybersecurity entails trade-offs between competing goods—and not just security versus privacy, although these are prominent examples<sup>29</sup>—that cannot be made intelligently unless the competing values are properly identified and assessed as to their relative importance. The result of what I am guessing is pervasive ignorance as to the actual stakes in the search for good cyber policy is an absence of any authoritative policy deliberation—within or beyond government—that can plausibly develop the kind of political consensus needed to move beyond “muddling through.”

---

24. The difficult issues presented are well-surveyed in NAT’L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 239–92 (William A. Owens et al. eds., 2009).

25. See *supra* text accompanying note 20.

26. HUNKER, *supra* note 16, at 119.

27. For a discussion of these intricate relationships, see Mark D. Young, *Cyber Operational Relationships in the United States Government*, 8 I/S: J.L. & POL’Y FOR INFO. SOC’Y (forthcoming 2012).

28. See Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEXAS L. REV. 1533, 1555 (2010) (recognizing the difficulty of cooperation between the President and private industry in this area). For a discussion of the role of public–private partnerships in cybersecurity, see Jeffrey Hunker, *Global Leadership in Cybersecurity: Can the U.S. Provide It?*, 8 I/S: J.L. & POL’Y FOR INFO. SOC’Y (forthcoming 2012).

29. Sean Kanuck, *Sovereign Discourse on Cyber Conflict Under International Law*, 88 TEXAS L. REV. 1571, 1590 (2010).

If I am right about the foundational problems, then Mr. Thompson's recommendations simply cannot take us very far in the right direction. First, there is his prescription for a single official—appointed with Senate advice and consent—to coordinate a streamlined cyber-policy process.<sup>30</sup> Representative Jim Langevin (D-R.I.) earlier this year proposed legislation along these lines to establish a National Office for Cyberspace in the Executive Office of the President.<sup>31</sup> The Director of that office would chair an interagency Federal Cybersecurity Practice Board.<sup>32</sup> Together, they would develop and police the implementation of policies to achieve “[g]overnmentwide protection of Government-networked computers against common attacks” and “agencywide protection against threats, vulnerabilities, and other risks to the information infrastructure within individual agencies.”<sup>33</sup> This is not necessarily a bad proposal (although it appears to be limited to protecting only government infrastructure).

However, our most recent experience with centralizing national security policy-making authority in a single official offers a rather disheartening precedent. In order to address the problem of bewildering complexity in the allocation of intelligence responsibilities, Congress, in 2004, authorized the creation of a new institution, the Office of the Director of National Intelligence (ODNI), which would have authority to bring the unwieldy intelligence sector under control<sup>34</sup>—addressing a problem closely resembling the current cybersecurity tangle. Yet, six years later, in a lengthy 2010 investigation, two *Washington Post* reporters concluded:

The top-secret world the government created in response to the terrorist attacks of Sept. 11, 2001, has become so large, so unwieldy and so secretive that no one knows how much money it costs, how many people it employs, how many programs exist within it or exactly how many agencies do the same work.<sup>35</sup>

Stunningly, the reporters found, “Some 1,271 government organizations and 1,931 private companies work on programs related to counterterrorism, homeland security and intelligence in some 10,000 locations across the United States.”<sup>36</sup> The ODNI's apparent failure to tame the bureaucratic beast presumably results from its lack of clear legal or budgetary authority with regard to the agencies within its supposed purview. Extrapolating from this example to the world of cybersecurity—and recognizing that the Secretaries

---

30. Thompson, *supra* note 1, at 489–91.

31. Executive Cyberspace Coordination Act of 2011, H.R. 1136, 112th Cong. (2011).

32. *Id.* § 101.

33. *Id.*

34. Intelligence Reform and Terrorism Prevention Act of 2004 § 1011, 50 U.S.C. § 403 (2006).

35. Dana Priest & William M. Arkin, *Top-Secret America: A Hidden World, Growing Beyond Control*, WASH. POST, July 19, 2010, available at <http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/>.

36. *Id.*

of Defense and Homeland Security are the two officials with the greatest relevant responsibility in this domain—there is likely to be no individual other than the President of the United States with enough leverage to bring order to the chaos. The President’s principal forum for making key decisions is—and ought to be—the National Security Council. Adding another official to the mix—unless that official has the heft and proximity to operate as the President’s personal alter ego—is unlikely to produce any positive effect. Senate advice and consent is all but certainly beside the point.

As for designing a “uniform federal authentication system . . . to verify, track, and control access to different portions of the federal network structure based on a standard security scheme,”<sup>37</sup> I cannot claim sufficient engineering expertise to know whether this is practicable, but it strikes me as problematic. The Department of Defense alone is responsible for maintaining over 15,000 computer networks.<sup>38</sup> The number of civilian networks for which the Department of Homeland Security (DHS) is responsible across the rest of the federal government is presumably much greater. Standardization across so vast a domain seems doubtful, to say the least. The government has never even been able to establish even a common look-and-feel for its websites.

But one wonders also whether standardization would be good policy. Here is where one of those policy trade-offs that seem rarely discussed might significantly come into play. It might be, for all I know, that a security scheme allowing verification, tracking, and access control to, say, the computers that monitor our nuclear arsenal could be installed on networks responsible for keeping crop data in the U.S. Department of Agriculture (USDA) without reducing the efficiency and productivity of the USDA workforce—or imposing significantly on the USDA budget. But I am guessing that the answer is negative. And if my guess is right that greater security imposes certain transaction costs on doing everyday business, then maybe the use of identical security processes on every federal computer network for its own sake is not the way to go—at least not without weighing the competing costs.

Furthermore, I assume that if all federal networks were subject to the same security scheme, breaking that system would effectively permit hacking the entire federal government. In discussing the case for standards in 2004, the Government Accountability Office wrote:

[T]he development and use of a standard can attract a scrutiny that helps to reduce design flaws and promote security. Additionally, the existence of standards promotes the availability of detailed technical information about a technology, which may serve as a basis for

---

37. Thompson, *supra* note 1, at 492.

38. Young, *supra* note 27.

determining where vulnerabilities remain. *At the same time, however, an attack against a specific standard-conforming technology can succeed against all systems that use the standard.* On the other hand, a single countermeasure could protect all standards-compliant systems. Thus, standards can help as well as hurt cybersecurity. Overall, standards would be useful in promoting cybersecurity because they would make it possible for organizations, including the federal government, to purchase cybersecurity technologies that meet minimum standards.<sup>39</sup>

Recognizing my own limited technical expertise in this area, I cannot help but wonder—in light of this cautious assessment—whether uniform “minimum standards,” rather than a “uniform federal authentication system,” is the way to go.

As for Point 5, Mr. Thompson’s discussion of the private sector is both somewhat inconsistent and altogether too modest. He touts the benefit of smart regulations—that is regulations that are “flexible” but “enforceable”—and then cautions that even these regulations must be “implemented judiciously to avoid overburdening both regulators and private sector entities.”<sup>40</sup> Quite interestingly, however, he then immediately moves to the first of two high priority regulatory targets and suggests a straightforward command-and-control technological requirement, i.e., air-gapping all “supercritical systems.”<sup>41</sup> My point in highlighting this inconsistency is not that Mr. Thompson is wrong about air-gapping; he might be right. My point is that starting the regulatory inquiry with an implicit antiregulatory bias may be counterproductive in contexts where “hard” and specific regulation is sensible.

His second suggestion, if I understand it correctly, is that tier-one ISPs are to be required in some flexible way to develop capacities for detecting and cutting off malicious traffic. This is well and good, as far as it goes—obviously, as Mr. Thompson notes,<sup>42</sup> there would need to be considerable regulatory oversight to prevent abuse—but it does not deal with a critical private-sector problem, which the National Research Council calls *cyberexploitation*.<sup>43</sup> As with espionage, its aim is to secure unauthorized access to confidential information, while allowing the computer system on

---

39. U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-04-321, TECHNOLOGY ASSESSMENT: CYBERSECURITY FOR CRITICAL INFRASTRUCTURE PROTECTION 52–3 (2004) (emphasis added), available at <http://www.gao.gov/assets/160/157541.pdf>.

40. Thompson, *supra* note 1, at 493–94.

41. *Id.* at 494. There is also an obvious tension between a smart-regulation approach to private networks and a recommendation that all federal networks implement a single, uniform security scheme.

42. *Id.*

43. See NAT’L RESEARCH COUNCIL, *supra* note 24, at 10–11 (identifying cyberexploitation as one of two types of hostile attacks on computer networks).

which that information resides to run normally.<sup>44</sup> Virtually every proposal to deal with cyberexploitation highlights the need for public–private partnerships, which, in certain sectors, have worked decently well.<sup>45</sup> In the financial sector, for example, where the government has significant leverage over the private firms (through SEC disclosure requirements, for example), and there is a long history of public–private interaction that has established a certain level of mutual trust, the public–private partnership model has reportedly worked reasonably.<sup>46</sup> In other areas, where no such groundwork exists, the public–private partnership idea has gone next to nowhere.<sup>47</sup>

And here is the nub of the problem. Part of our cybersecurity problem is institutional—we do not have organizations and practices in place to provide anything like efficient and effective governance in the cybersecurity area. But another huge part is regulatory. We simply do not have in place a framework of laws and regulations, “smart” or otherwise, that adequately incentivizes the parties with the greatest capacity to improve our security to do so.<sup>48</sup> Achieving cybersecurity is a classic collective-action problem, where everyone doing his or her personal best under some loosely defined common objectives is not going to produce an optimal result.<sup>49</sup> There has to be a coordinated, enforceable policy and regulatory framework backed by adequate public investment to achieve the public good.

What this means, in turn, is that the public good with regard to cybersecurity needs to be defined. It cannot be perfect security—no such thing exists. It cannot be security at all costs—there are other public goods for which we must pay. It must be a set of security goals that is sensible given the inevitable trade-offs among security, privacy, productivity, economic growth, organizational flexibility, military effectiveness, government transparency, and accountability—all goals we care about. And there must be a sensible evaluation of risk—an evaluation that is currently bedeviled by incomplete statistics and data gathering.<sup>50</sup>

---

44. *Id.* at 11.

45. See Hunker, *supra* note 28 (describing a successful public–private approach to Y2K, whereby the United States government required private companies to report what precautions they had taken but allowed them to decide which precautions were appropriate).

46. See, e.g., William W. Bratton, *Private Standards, Public Governance: A New Look at the Financial Accounting Standards Board*, 48 B.C. L. REV. 5, 52–53 (2007) (arguing that the public–private Financial Accounting Standards Board is a “second best” solution, although nothing better has emerged in its stead).

47. See Hunker, *supra* note 28 (observing that security plans for commercial facilities rank among the worst).

48. HUNKER, *supra* note 16, at 131–33.

49. See DENNIS CHONG, *COLLECTIVE ACTION AND THE CIVIL RIGHTS MOVEMENT* 6 (1991) (“[A] collective action problem arises whenever individuals arrive at strictly Pareto-inferior outcomes in the pursuit of their self-interest.” (citation omitted)).

50. Herbert Lin, *Thoughts on Threat Assessment in Cyberspace*, 8 I/S: J.L. & POL’Y FOR INFO. SOC’Y (forthcoming 2012).

I do not believe any such policy framework can result from the current state of public ignorance of or indifference to this issue. On the very first page of its April 2009 *Cyberspace Policy Review*, the White House declared, “The United States needs to conduct a national dialogue on cybersecurity to develop more public awareness of the threat and risks and to ensure an integrated approach toward the Nation’s need for security and the national commitment to privacy rights and civil liberties guaranteed by the Constitution and law.”<sup>51</sup> This is absolutely true. Galvanizing such a dialogue, however, requires some high profile mechanism for raising the visibility of the issue and eliciting broad-based discussion that goes beyond the usual Washington venues. The traditional tool for such an initiative is a blue-ribbon national commission, like the 9/11 Commission,<sup>52</sup> the Carnegie Commission that led to the creation of the Corporation for Public Broadcasting,<sup>53</sup> or the Kerner Commission that looked into the causes of the 1960s race riots in the United States.<sup>54</sup> In a forthcoming article, I lay out a scenario by which such a commission could elicit genuine deliberative participation from a broad, nonexpert public so that its ultimate recommendations reflect both technical expertise and democratic input.<sup>55</sup> I believe that only such an initiative—which looks at cybersecurity through the eyes of everyone whose interests are implicated—will be adequate to produce the sort of political movement that can produce significant change.

I am not certain, of course, whether my proposal is sufficient or whether a national commission on this topic is politically feasible. I am confident, however, that, without a broad-based national conversation that looks beyond the kill switch debate to all the public values involved, we are not going to get the regulatory framework or public investment that will engender real security.

---

51. WHITE HOUSE, *CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE*, at i, available at [http://www.whitehouse.gov/assets/documents/Cyberspace\\_Policy\\_Review\\_final.pdf](http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf).

52. For the findings of this effort, see NAT’L COMM’N ON TERRORIST ATTACKS UPON THE U.S., *FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES* (2004).

53. CARNEGIE COMM’N ON EDUC. TELEVISION, *PUBLIC TELEVISION: A PROGRAM FOR ACTION—THE REPORT AND RECOMMENDATIONS OF THE CARNEGIE COMMISSION ON EDUCATIONAL TELEVISION* (1967).

54. NAT’L ADVISORY COMM’N ON CIVIL DISORDERS, *REPORT OF THE NATIONAL ADVISORY COMMISSION ON CIVIL DISORDERS* (1968).

55. Peter M. Shane, *Cybersecurity Policy as if “Ordinary Citizens” Mattered: The Case for Public Participation in Cyber Policy Making*, 8 I/S: J.L. & POL’Y FOR INFO. SOC’Y (forthcoming 2012).