Articles

Public-Private Cybersecurity

Kristen E. Eichensehr*

Calls for public-private partnerships to address U.S. cybersecurity failures have become ubiquitous. But the academic literature and public debate have not fully appreciated the extent to which the United States has already backed into a de facto system of "public-private cybersecurity." This system is characterized by the surprisingly important, quasi-governmental role of the private sector on key cybersecurity issues, and correspondingly by instances in which the federal government acts more like a market participant than a traditional regulator. The public-private cybersecurity system challenges scholarly approaches to privatization, which focus on maintaining public law values when government functions are contracted out to private parties. The informal and complicated structure of public-private relationships in cybersecurity renders concerns about public law values at once more serious and more difficult to remedy.

This Article first explores the line between public and private functions and provides a descriptive account of the public-private cybersecurity system. It highlights the relative roles of the U.S. government and private sector in four important contexts related to international cybersecurity threats: (1) disrupting networks of infected computers used by transnational-criminal groups ("botnet takedowns"), (2) remediating software vulnerabilities that can be used for crime, espionage, and offensive operations ("zero-day vulnerabilities"), (3) attributing cyber intrusions to state-sponsored attackers, and (4) defending privately-owned systems and networks from sophisticated, nation-state-sponsored attackers.

The Article then uses the public-private cybersecurity system to challenge and complicate existing scholarship on privatization. Procedurally, the public-

---

* Assistant Professor, UCLA School of Law. For helpful conversations and comments on earlier drafts, I am grateful to Tendayi Achiume, Sam Bray, Fred Cate, Anupam Chander, Beth Colgan, Sharon Dolovich, Mark Grady, Jennifer Granick, Duncan Hollis, Herb Lin, Jon Michaels, Paul Ohm, Ted Parson, Kal Raustiala, Condoleezza Rice, Richard Re, Sidney Tarrow, Amy Zegart, and participants in the Hoover Institution Summer Security Fellows Workshop, Cornell International Law/International Relations Workshop, American Society of International Law Midyear Research Forum, and AALS National Security Law Section Works-in-Progress session. Thanks to UCLA School of Law and the Hoover Institution for research support and to Andrew Brown, Danielle Hesse, Vincent Marchetta, and Kevin Whitfield for excellent research assistance. This Article reflects developments through January 2017, when it was finalized for publication.

private cybersecurity system differs from traditional privatization because private actors—not the government—decide what functions they should perform, and private actors operate outside of the contractual frameworks that have traditionally restrained private contractors. Substantively, the cybersecurity context implicates public law values addressed in prior work—including accountability, transparency, and due process or fairness—but it also raises additional concerns about security and privacy.

Evaluating how the public-private cybersecurity system attains and falls short of public law values yields broader lessons for cybersecurity governance and for privatization. The public-private cybersecurity system shows that concerns about public law values are not unidirectional—sometimes threats to public values come from the government, not the private sector. On the other hand, while empowered private parties play a crucial role in cybersecurity and in many ways currently support public values, this alignment is a present fortuity, not a structural feature, and so may shift in the future, posing new threats to public law values. These complexities require new kinds of context-dependent solutions to safeguard public law values. The Article concludes by suggesting several such remedies for the public law failings it identifies.

Introduction

[N]either government, nor the private sector can defend the nation alone. It's going to have to be a shared mission—government and industry working hand in hand, as partners.

—Barack Obama, Remarks at the National Cybersecurity Communications Integration Center, January 13, 2015[1]

Calls to establish public-private partnerships in cybersecurity have become ubiquitous.[2] From government officials[3] to private sector

1. President Barack Obama, Remarks by the President at the National Cybersecurity Communications Integration Center (Jan. 13, 2015), https://www.whitehouse.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent [https://perma.cc/ENG2-GG4G].

2. BENJAMIN WITTES & GABRIELLA BLUM, THE FUTURE OF VIOLENCE: ROBOTS AND GERMS, HACKERS AND DRONES 74 (2015) ("[S]o pervasive is the understanding that the private sector has a key role to play in cybersecurity that the term 'public-private partnership' has become a cliché in the cybersecurity world.").

3. *See, e.g.*, President Barack Obama, Remarks by the President at the Cybersecurity and Consumer Protection Summit (Feb. 13, 2015), https://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit [https://perma.cc/5LZC-95MA] ("There's only one way to defend America from these cyber threats, and that is through government and industry working together, sharing appropriate information as true partners."); Press Release, U.S. Dep't of Homeland Sec., Statement by Secretary Jeh C. Johnson Regarding PPD-41, Cyber Incident Coordination (July 26, 2016), https://www.dhs.gov/news/2016/07/26/statement-secretary-jeh-c-johnson-regarding-ppd-41-cyber-incident-coordination [https://perma.cc/P8D6-DG7C] (explaining that Presidential Policy Directive 41 "re-enforces the reality that cybersecurity must be a partnership between the government and the private sector").

representatives,[4] think tanks,[5] expert commissions,[6] and the media,[7] "partnership" has become the watchword for remedying cybersecurity failures in the United States.[8]

But the academic literature and public debate have not fully appreciated the extent to which the United States has already backed into a de facto system of "public-private cybersecurity."[9] The public-private cybersecurity system is characterized by the surprisingly important, quasi-governmental

---

4. *See, e.g.*, SCOTT CHARNEY ET AL., MICROSOFT, FROM ARTICULATION TO IMPLEMENTATION: ENABLING PROGRESS ON CYBERSECURITY NORMS 13 (2016), https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms_vFinal.pdf [https://perma.cc/8PF2-VBX5] ("Public/private partnerships will be the anvil on which we forge the cybersecurity norms to protect the foundations of the 21st century in cyberspace.").

5. *See, e.g.*, CSIS COMM'N ON CYBERSECURITY FOR THE 44TH PRESIDENCY, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 2 (2008), http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf [https://perma.cc/43GL-ENB6] ("Government must recast its relationship with the private sector as well as redesign the public-private partnership to promote better cybersecurity.").

6. *See* COMM'N ON ENHANCING NAT'L CYBERSECURITY, REPORT ON SECURING AND GROWING THE DIGITAL ECONOMY 13 (2016), https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf [https://perma.cc/VM98-5RHN] ("[N]either the government nor the private sector can capably protect systems and networks without extensive and close cooperation.").

7. *See, e.g.*, Editorial, *Better Cybersecurity Defenses Require a Concerted Public-Private Effort*, WASH. POST (Jan. 15, 2015), https://www.washingtonpost.com/opinions/better-cybersecurity-defenses-require-a-concerted-public-private-effort/2015/01/15/ba585cb8-9c2d-11e4-96cc-e858eba91ced_story.html [https://perma.cc/E4FP-7PXV].

8. *See, e.g.*, Alejandro Mayorkas, Deputy Sec'y of Homeland Sec., U.S. Dep't of Homeland Sec., Remarks by Deputy Secretary Alejandro Mayorkas at the 6th Annual International Cybersecurity Conference (June 20, 2016), https://www.dhs.gov/news/2016/06/22/remarks-deputy-secretary-alejandro-mayorkas-6th-annual-international-cybersecurity [https://perma.cc/3A4A-SGFR] (discussing the Department of Homeland Security's role in building a "public-private partnership" for cybersecurity information sharing); *Microsoft, Financial Services and Others Join Forces to Combat Massive Cybercrime Ring*, MICROSOFT (June 5, 2013), http://news.microsoft.com/2013/06/05/microsoft-financial-services-and-others-join-forces-to-combat-massive-cybercrime-ring/ [https://perma.cc/SBA3-AZ3Z] (quoting Federal Bureau of Investigation (FBI) Executive Assistant Director Richard McFeely, stating that "[c]reating successful public-private relationships . . . is the ultimate key to success in addressing cyber threats and is among the highest priorities of the FBI").

9. Commentators are increasingly acknowledging the convergence of governmental and private roles in cybersecurity. *See, e.g.*, ADAM SEGAL, THE HACKED WORLD ORDER: HOW NATIONS FIGHT, TRADE, MANEUVER, AND MANIPULATE IN THE DIGITAL AGE 17 (2016) ("[T]he battle over cyberspace is remaking the division between the public and the private."); WITTES & BLUM, *supra* note 2, at 79 (noting the "migration in law, practice, and custom of important security functions—surveillance, analysis, interception . . . —from government to private actors"); Samuel J. Rascoff, *The Norm Against Economic Espionage for the Benefit of Private Firms: Some Theoretical Reflections*, 83 U. CHI. L. REV. 249, 266 (2016) ("[C]ybersecurity tends to require ever-greater blurring of the boundaries between public and private actors in the provision of national security."). This Article is the first to propose conceptualizing the U.S. approach to cybersecurity governance as a public-private system and the first to analyze how existing literature on privatization and public law values can be adapted to the new, complex public-private cybersecurity context.

role of the private sector on many important cybersecurity issues, and correspondingly, by instances in which the federal government acts more like a market participant than a traditional regulator. For example, private companies investigate networks of malware-infected computers that are used by transnational criminal groups for financial fraud, obtain judicial orders allowing them to seize control of the networks, and work with Internet service providers to eliminate malware infections on individuals' computers.[10] The federal government, on the other hand, has become a literal market participant by purchasing software vulnerabilities on the black market and sometimes failing to disclose them to software makers that could remedy the flaws.[11]

Although the public-private cybersecurity system includes government-like roles for the private sector, it differs from privatization in the traditional sense. Privatization is often understood to be synonymous with the government contracting out governmental functions.[12] Under that model, the government formally signs up a private company as an agent to carry out functions that the government itself previously performed and then supervises the private party's performance of the actions.[13] By contrast, the public-private system that this Article addresses occurs informally. In some circumstances, private companies have stepped in independently to remedy cybersecurity problems out of frustration with the government's failure to act.[14] In other circumstances, private companies act as a force multiplier, cooperating with the government to undertake cybersecurity operations.[15] In still other circumstances, the government seems to have informally encouraged and even assisted private parties in doing things that the government does not want to do itself, but which it nevertheless finds useful. For example, the federal government has reportedly provided information on cyber intrusions to companies that then attribute breaches to foreign countries, even when the government refuses to identify the perpetrator officially.[16]

The public-private cybersecurity system has accreted over time as a jury-rigged response to perceived security failures and market opportunities,

---

10. *See infra* section I(B)(1).

11. *See infra* section I(B)(2).

12. *See infra* notes 183–84 and accompanying text.

13. Of course, lack of government supervision in practice has caused serious concerns in some cases. For just one example, see James Risen, *Before Shooting in Iraq, a Warning on Blackwater*, N.Y. TIMES (June 29, 2014), http://www.nytimes.com/2014/06/30/us/before-shooting-in-iraq-warning-on-blackwater.html?_r=0 [https://perma.cc/5RBB-4HSW] (detailing lack of oversight of the security contractor, Blackwater, in Iraq prior to the shooting of seventeen civilians in Nisour Square in 2007).

14. *See infra* section I(B)(4).

15. *See infra* notes 165–69 and accompanying text.

16. *See, e.g.*, *infra* note 120 and accompanying text.

and it has developed without democratic deliberation or even much public awareness. The system evolved without going through the usual processes of public, governmental decision making, and because of its informality, it has also remained largely outside the scope of after-the-fact mechanisms for checking governmental actions, including, for example, congressional hearings.[17] These features of the de facto public-private cybersecurity system create risks that it may not effectuate the public law values, such as accountability and fairness, that the normal, formal processes of government functioning are designed to foster.

This Article contributes to debates about cybersecurity and privatization more broadly in three ways.

Part I explores the line between public and private functions and argues that transnational crime control, foreign policy, and national security are quintessentially "public," or governmental, functions that implicate public law values. Part I then provides a descriptive account of the public-private cybersecurity system, exploring some of the most important and contested cybersecurity issues to show how governmental and private roles are blurring and in some instances reversing. In particular, Part I examines four case studies related to significant international cybersecurity threats that implicate arguably public functions: (1) disrupting networks of infected computers used by transnational criminal groups for malicious purposes ("botnet takedowns"), (2) remediating software security vulnerabilities that can be used for crime, espionage, and offensive governmental operations ("zero-day vulnerabilities"), (3) attributing cyber intrusions to state-sponsored attackers, and (4) defending privately owned systems and networks against sophisticated, nation-state-sponsored attackers. Examples within each case study show the diversity of private sector–government relationships, ranging from declared partnerships to largely independent, but mutually beneficial, actions to overtly adversarial clashes.

Part II uses the public-private cybersecurity system to challenge and complicate existing scholarship on privatization. Despite the similarity of private parties performing arguably governmental functions, the public-private cybersecurity system differs from existing understandings of privatization in ways that suggest different safeguards may be needed in the cybersecurity context.

As a procedural matter, the public-private cybersecurity system differs from traditional contracting out because the private actors—not the government—decide at the outset what functions they should perform, and the private actors operate outside of the contractual frameworks that

17. *See* Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 924–25 (2008) (describing similar oversight gaps for informal intelligence partnerships).

governments have used to restrain private contractors in other circumstances. As a substantive matter, the cybersecurity context raises concerns about public law values that have been the focus of prior work—including accountability, transparency, and due process or fairness—but it also engages additional concerns about optimal provision of security and protection of privacy.

Finally, Part III uses a preliminary evaluation of how the public-private cybersecurity system attains and falls short of public law values to draw broader lessons for cybersecurity and privatization going forward. In particular, the public-private cybersecurity system shows that concerns about public law values are not unidirectional. This is not a simple story of a public values-minded government reining in wayward private contractors. Sometimes the government is absent, and sometimes it is the source of threats to public law values. On the other hand, although empowered private parties are crucial to how the public-private cybersecurity system functions and in many ways currently support public law values, this alignment is a present fortuity, not a structural feature, and may change in the future, posing additional challenges to public law values. Moreover, these complexities of the public-private cybersecurity system require changes to the nature of remedies for public law-values concerns and will require highly context-dependent solutions going forward. Part III suggests several such solutions to the specific public law failings it identifies.

The Article's discussion of public-private collaborations and role reversals is designed to be exemplary, rather than exhaustive. Comprehensiveness would be impossible in this area where secrecy is prevalent and transparency is lacking due to national security concerns and to the very informality of the system that the Article identifies. Rather, the Article builds out examples of government–private sector relationships on cybersecurity issues with an international component to show how cybersecurity is remaking those relationships and to demonstrate the insufficiency of existing theories about the role of private actors in public, governmental functions. By complicating existing understandings of privatization, the Article develops a more robust intellectual framework for conceptualizing unconventional public-private relationships and for ensuring that, despite new complexities, public law values can be protected going forward.

From the perspective of public values, the de facto, informal public-private cybersecurity system is neither wholly good nor wholly bad. Neither are the actors within it. Sometimes surprising patrons protect public law values in unexpected ways. But the system is complicated and will require context-dependent solutions to novel relationships that will continue to evolve as both the government and the private sector attempt to improve cybersecurity.

I. De Facto Public-Private Cybersecurity

Cybersecurity has sparked numerous examples of surprising relationships and collaboration between the government and the private sector, as well as role reversals.[18] This Article focuses on four manifestations of the public-private cybersecurity system that relate to international threats, either from transnational criminal groups, foreign government-sponsored private actors, or foreign governments themselves. The case studies focus on significant cybersecurity concerns that implicate at least arguably public functions. The selected case studies are also particularly useful illustrations of the complicated public-private interactions that are currently occurring. Focusing on this subset of public-private relationships helps to isolate what is public about what the private sector is doing and to illustrate the blurring of public and private functions in the cybersecurity context.

Subpart I(A) explores the nature of public and private functions as they relate to transnational crime, national defense, and foreign policy. Subpart I(B) uses four case studies to argue that the United States currently has a de facto system of public-private cybersecurity, although one more nuanced and complicated than traditional understandings of privatization or formal public-private partnerships. Subpart I(C) explores the incentives that drive both the U.S. government and the private sector to undertake their respective roles in the public-private cybersecurity system.

---

18. "Cybersecurity" is a capacious concept, susceptible to varying definitions. *See, e.g.*, *Global Cyber Definitions Database*, NEW AMERICA CYBER SECURITY INITIATIVE, http://cyberdefinitions.newamerica.org/ [https://perma.cc/H3K9-YC9S] (collecting governmental and nongovernmental definitions of "cyber security" and related terms). For purposes of this Article, I understand "cybersecurity" as the process of protecting the confidentiality, integrity, and availability of information by preventing, detecting, and responding to attacks. This definition is a combination of definitions used by the U.S. National Institute of Standards and Technology and the International Organization for Standardization (ISO). *See* NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 37 (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf [https://perma.cc/CR46-RC6S] (defining "cybersecurity" as "[t]he process of protecting information by preventing, detecting, and responding to attacks"); *ISO/IEC 27032:2012*, INT'L ORG. FOR STANDARDIZATION, at 4.20, https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en [https://perma.cc/BD3R-FM9Z] (defining "cybersecurity" as "preservation of confidentiality, integrity and availability of information in the Cyberspace"). By focusing on security threats *to* information, this definition brackets, for purposes of this Article, security threats *from* information. The respective roles of governments and nongovernmental entities with regard to content-related security threats, such as use of the Internet by extremist groups, raise interesting and potentially different issues from their roles in cybersecurity as I have defined it here. *See, e.g.*, David P. Fidler, *Countering Islamic State Exploitation of the Internet*, COUNCIL ON FOREIGN REL. (2015), http://www.cfr.org/cybersecurity/countering-islamic-state-exploitation-internet/p36644?cid=otr-marketing-use-Islamic_State_cyber_brief [https://perma.cc/J4JG-XBQU] (discussing First Amendment issues related to countering the Islamic State's use of the Internet).

A. The Public-Private Divide

The public-private cybersecurity system described in this Part involves the blurring of public and private roles and even instances of role reversals in which private parties act quasi-governmentally and federal government actors appear more like private parties. These characterizations assume that certain activities are public and others are private.

At a conceptual level, the manifestations of public-private cybersecurity discussed in the following subpart involve, individually or in combination, transnational crime control, conduct of foreign policy, and provision of national defense. Botnets are often operated by transnational criminal groups, and botnet operators have been criminally charged in connection with botnet takedown operations.[19] Zero-day software vulnerabilities are used by governments to conduct espionage[20] and even offensive operations. The Stuxnet operation against Iranian nuclear facilities, for example, used five zero-day exploits.[21] Accusing foreign governments of hacking into U.S. companies has clear foreign-relations implications and also possible criminal consequences.[22] Defending targets within U.S. territory against nation-state or nation-state-sponsored attacks sounds like traditional national defense.

Each of these activities—crime control, foreign policy, and national defense—closely relates to the modern understanding that the state's function is to monopolize the legitimate use of force within a territory and to protect its citizens from both internal and external threats.[23] National defense and

---

19. *See, e.g.*, Indictment, United States v. Bogachev, No. 14-127 (W.D. Pa. May 19, 2014), http://www.justice.gov/sites/default/files/opa/legacy/2014/06/02/pittsburgh-indictment.pdf [https://perma.cc/3293-66RF] (listing charges against defendant for administering a botnet); Press Release, U.S. Dep't of Justice, U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator (June 2, 2014), http://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware [https://perma.cc/WKP7-HNFP] (discussing the criminal indictment of Russian citizen Evgeniy Bogachev for his role as a botnet administrator).

20. *See, e.g.*, Adam Entous & Danny Yadron, *Spy Virus Linked to Israel Targeted Hotels Used for Iran Nuclear Talks*, WALL STREET J. (June 10, 2015), http://www.wsj.com/articles/spy-virus-linked-to-israel-targeted-hotels-used-for-iran-nuclear-talks-1433937601 [https://perma.cc/49KA-RQ9W] (reporting on an improved version of the Duqu virus that used zero-day exploits to compromise hotels where Iranian nuclear negotiations were held).

21. Kim Zetter, *US Used Zero-Day Exploits Before It Had Policies for Them*, WIRED (Mar. 30, 2015), http://www.wired.com/2015/03/us-used-zero-day-exploits-policies/ [https://perma.cc/TU9S-JL9B].

22. *See infra* note 296 and accompanying text.

23. *See* Max Weber, *Politics as a Vocation*, *in* FROM MAX WEBER: ESSAYS IN SOCIOLOGY 77, 78 (H. H. Gerth & C. Wright Mills eds., 1946) ("[A] state is a human community that (successfully) claims the *monopoly of the legitimate use of physical force* within a given territory. . . . Specifically, . . . the right to use physical force is ascribed to other institutions or to individuals only to the extent to which the state permits it."); *see also* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 312 (1972) (noting that "[i]t has been said that '[t]he most basic function of any government is to provide for the security of the individual and of his property,'" and arguing that

foreign policy are frequently cited as the quintessential examples of governmental, or public, functions.[24] Crime control and law enforcement are often placed in the same category of activities that are historically or necessarily public.[25]

Scholars argue that functions like national defense and foreign policy are so core to the purpose or nature of government that they cannot legitimately be performed by private parties.[26] Such activities "go to the heart of . . . the state's inherent responsibilities in a liberal democratic society,"[27] and "the duty to be accountable for public decisions is not a function performable by those outside government."[28] Allowing private actors to perform such functions "challenges the role of government and the rule of law that sustains it."[29]

"unless Government safeguards its own capacity to function and to preserve the security of its people, society itself could become so disordered that all rights and liberties would be endangered" (citation omitted)); David A. Sklansky, *The Private Police*, 46 UCLA L. REV. 1165, 1188 (1999) (noting the view that "the very point of government is to monopolize the coercive use of force, in order to ensure public peace, personal security, and the use and enjoyment of property").

24. *See, e.g.*, JOHN D. DONAHUE & RICHARD J. ZECKHAUSER, COLLABORATIVE GOVERNANCE: PRIVATE ROLES FOR PUBLIC GOALS IN TURBULENT TIMES 20 (2011) (arguing, within the context of advocating "collaborative governance" in general, that "[s]ome public functions—imposing taxes, engaging in diplomacy, and conducting military operations—are best left as exclusively governmental activities"); Laura A. Dickinson, *Public Law Values in a Privatized World*, 31 YALE J. INT'L L. 383, 390 (2006) ("Probably no function of government is deemed more quintessentially a 'state' function than the military protection of the state itself . . . ."); Jody Freeman, *Extending Public Law Norms Through Privatization*, 116 HARV. L. REV. 1285, 1300 (2003) (noting that ideological opposition to privatization for some is "limited to activities where privatization seems unfathomable (such as foreign policy or national defense)").

25. Elizabeth E. Joh, *Conceptualizing the Private Police*, 2005 UTAH L. REV. 573, 585 (noting that after the establishment of public policing, "the activity of policing became identified primarily as a government function"); Sklansky, *supra* note 23, at 1168 ("[M]aintaining order and controlling crime are paradigmatic government functions . . . ."); David Alan Sklansky, Essay, *Private Police and Democracy*, 43 AM. CRIM. L. REV. 89, 89 (2006) ("For most people, the police are government incarnate: the street-level embodiment of the state's monopolization of legitimate force.").

26. *See, e.g.*, Dickinson, *supra* note 24, at 390 ("[S]ome scholars of privatization in the domestic sphere have assumed that the military is one area where privatization does not, or should not, occur."); Oliver Hart et al., *The Proper Scope of Government: Theory and an Application to Prisons*, 112 Q.J. ECON. 1127, 1155, 1158 (1997) (citing foreign policy and the armed forces as examples in which privatization would be problematic); Sidney A. Shapiro, *Outsourcing Government Regulation*, 53 DUKE L.J. 389, 417–18 (2003) (citing foreign affairs as an area that cannot be privatized); Michael J. Trebilcock & Edward M. Iacobucci, *Privatization and Accountability*, 116 HARV. L. REV. 1422, 1444 (2003) (citing "the formulation and implementation of a country's foreign or defense policy" as examples of instances in which the "complexity of objectives and unforeseeable contingencies render delegations of these functions to private actors highly problematic").

27. Freeman, *supra* note 24, at 1295 (characterizing the views of some privatization opponents).

28. Paul R. Verkuil, *Public Law Limitations on Privatization of Government Functions*, 84 N.C. L. REV. 397, 425–26 (2006).

29. *Id.* at 419.

The U.S. federal government ostensibly protects against this concern through a process formalized in Office of Management and Budget Circular No. A-76.[30] The circular instructs federal agencies to identify each of their activities as "either commercial or inherently governmental" and to "[p]erform inherently governmental activities with government personnel."[31] Commercial activities, on the other hand, may be outsourced to private actors pursuant to specific procedures.[32] Circular A-76 defines "inherently governmental activity" as "an activity that is so intimately related to the public interest as to mandate performance by government personnel."[33] It further explains that such activities "require the exercise of substantial discretion in applying government authority and/or in making decisions for the government."[34]

Despite Circular No. A-76's apparent limitation on privatization, the circular's efficacy is highly questionable. Its on-paper restrictions have proven pliable in practice. For example, during the recent conflicts in Iraq and Afghanistan, private military contractors often outnumbered U.S. military personnel,[35] and some commentators have inferred from "the extensive use of private contractors in Iraq and Afghanistan, for everything from food service to security to interrogation of prisoners, . . . that there are in practice apparently no limits to the important governmental functions that may be contracted out."[36]

---

30. OFFICE OF MGMT. & BUDGET, CIRCULAR NO. A-76 REVISED, attachment A, § B(1) (2003), https://www.whitehouse.gov/omb/circulars_a076_a76_incl_tech_correction/ [https://perma.cc/YVE9-QUE5].

31. *Id.* § 4(a)–(b).

32. *Id.* at attachment B.

33. *Id.* at attachment A, § B(1)(a).

34. *Id.* The Circular provides examples, including "[d]etermining, protecting, and advancing economic, political, territorial, property, or other interests by military or diplomatic action, civil or criminal judicial proceedings, contract management, or otherwise." *Id.* at attachment A, § B(1)(a)(2). The Federal Activities Inventory Reform Act (FAIR Act) codifies a similar definition of "inherently governmental function." 31 U.S.C. § 501 note § 5(2)(A) (2012).

35. MOSHE SCHWARTZ & JOYPRADA SWAIN, CONG. RESEARCH SERV., DEPARTMENT OF DEFENSE CONTRACTORS IN AFGHANISTAN AND IRAQ: BACKGROUND AND ANALYSIS 1–2 (2011), https://www.fas.org/sgp/crs/natsec/R40764.pdf [https://perma.cc/A2HY-YJEU] (providing data to show that in U.S. operations in Iraq, Afghanistan, and the Balkans, "contractors have comprised approximately 50% of DOD's . . . workforce in country"); Micah Zenko, *The New Unknown Soldiers of Afghanistan and Iraq*, FOREIGN POL'Y (May 29, 2015), http://foreignpolicy.com /2015/05/29/the-new-unknown-soldiers-of-afghanistan-and-iraq/ [https://perma.cc/SA3S-4JUN] (reporting on data showing that since 2008, contractors outnumbered U.S. military forces in Iraq and Afghanistan).

36. Dominique Custos & John Reitz, *Public-Private Partnerships*, 58 AM. J. COMP. L. (SUPP.) 555, 582 (2010).

Even supposedly quintessential governmental activities have not proven to be necessarily or immutably public.[37] For example, the nature of policing has shifted over time from private to public,[38] to the public-private mixture in the United States today, where "private guards greatly outnumber sworn law enforcement officers."[39] The use of private military contractors has followed a similar trajectory. In cybersecurity, as in other contexts, the roles and responsibilities of governmental and private actors may shift over time across a permeable public-private divide.[40]

Nonetheless, consistent with the notion that crime control, foreign policy, and national defense have public aspects, the performance of these functions by private actors in the cybersecurity context triggers a need for scholarly investigations similar to those that have occurred for private performance of other traditionally public functions. Better understanding the public nature of functions performed by private parties and the potentially nonpublicized nature of some governmental actions can enable more thoughtful, deliberate decisions about who should undertake particular functions and how.

B. Manifestations of Public-Private Cybersecurity

Using four case studies, this subpart argues as a descriptive matter that a mixed public-private cybersecurity system currently operates in the United States. The case studies illustrate the blurring of the public-private divide, providing examples where private parties act to support public values, and government actors behave less like public authorities than like private actors.

This Article speaks of a public-private cybersecurity *system*, rather than a public-private partnership, because the case studies show that the private sector and government do not always act as partners. Sometimes they are antagonists, and sometimes their relationship is ambiguous at best. Specific

---

37. *Cf.* Sklansky, *supra* note 25, at 89 (explaining that "there was nothing natural or inevitable about the displacement of private guards and detectives by public police" and that "[s]tarting in the 1970s, growth in public law enforcement slackened, and the private security industry exploded").

38. For a history of the evolution of private and public policing, see Sklansky, *supra* note 23, at 1193–221.

39. Sklansky, *supra* note 25, at 89.

40. *Cf.* SEGAL, *supra* note 9, at 110 ("The current division of responsibility for cybersecurity between the government and the private sector is not firmly set . . . . A destructive attack could easily result in a shift toward greater government intervention . . . . Or in response to future revelations about NSA surveillance, the technology companies may chart an even more independent path . . . ."); MATT OLSON ET AL., BERKMAN CTR. FOR INTERNET & SOC'Y, DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK" DEBATE 9 (2016), https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [https://perma.cc/MA5Y-UBHY] (noting that U.S. companies "are increasingly playing a quasi-sovereign role as they face difficult decisions when foreign government agencies pressure them to produce data about citizens abroad").

examples within the case studies show how even within a particular issue area, the private sector's relationship with the government can vary from declared partnership to largely independent but mutually beneficial pursuit of each party's interests to overtly adversarial clashes.

1. Botnet Takedowns.—In the past few years, the private sector and law enforcement agencies have collaborated to engage in "botnet takedowns." "Botnets" (short for "robot networks") are networks of computers that are infected with malicious software that allows "bot herders" to control the computers remotely.[41] Botnets can be used for a variety of malicious activity, such as sending spam, launching denial-of-service attacks that disable websites, and stealing credit card or other information that bot herders use to commit financial fraud.[42] Actions to eliminate bot herders' control of botnets are called "takedowns."[43]

Although the crimes perpetrated using botnets may seem like a law enforcement concern, a private company undertook the first botnet takedown in the United States. In February 2010, Microsoft "launched a novel legal assault" to take down the Waledac botnet, which distributed spam.[44] Microsoft filed a civil suit under seal in federal district court against the unidentified individuals who controlled the botnet, arguing that the botnet, which targeted Microsoft's Windows operating system and Hotmail email service, harmed Microsoft and its customers.[45] Among other claims, Microsoft alleged that the botnet operators accessed computers belonging to Microsoft and its customers without authorization in violation of the Computer Fraud and Abuse Act and infringed Microsoft's trademark in violation of the Lanham Act.[46] The district court granted an ex parte temporary restraining order permitting Microsoft to initiate the deactivation

41. For an overview of botnets and how they work, see, for example, *Bots and Botnets—A Growing Threat*, NORTON, http://us.norton.com/botnet/ [https://perma.cc/L9FN-VRSA], and *Botnets 101: What They Are and How to Avoid Them*, FED. BUREAU OF INVESTIGATION (June 5, 2013), http://wayback.archive.org/web/20160629113903/https://www.fbi.gov/news/news_blog/botnets-101/botnets-101-what-they-are-and-how-to-avoid-them/ [https://perma.cc/U7HM-VST9].

42. *See, e.g.*, Zach Lerner, Note, *Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets*, 28 HARV. J.L. & TECH. 237, 238–42 (2014) (providing an overview of malicious activities conducted by botnets); Sam Zeitlin, Note, *Botnet Takedowns and the Fourth Amendment*, 90 N.Y.U. L. REV. 746, 748–51 (2015) (same).

43. *See, e.g.*, Tim Cranton, *Cracking Down on Botnets*, MICROSOFT (Feb. 24, 2010), http://blogs.microsoft.com/blog/2010/02/24/cracking-down-on-botnets/ [https://perma.cc/HZU7-R72E] (discussing botnet takedown operations).

44. *Id.*; Nick Wingfield & Ben Worthen, *Microsoft Battles Cyber Criminals*, WALL STREET J. (Feb. 26, 2010), http://www.wsj.com/articles /SB10001424052748704240004575086523786147014 [https://perma.cc/AYD8-NTTP].

45. Complaint at paras. 34–39, Microsoft Corp. v. John Doe, No. 1:10-cv-00156 (E.D. Va. Feb. 22, 2010).

46. *Id.* at paras. 40–45, 63–74.

of Internet addresses linked to the botnet, and thereby "sever[] the connection between the command and control centers of the botnet" and the infected computers.[47] A few months later, the court issued a final default judgment, ordering the permanent transfer of the Internet addresses to Microsoft.[48]

More than a year later, the U.S. government undertook its first botnet takedown, using tactics similar to Microsoft's and employing what Deputy Attorney General James M. Cole later called "creative lawyering."[49] The United States filed a civil suit in federal district court against the operators of the "Coreflood" botnet, alleging violations of wire fraud and bank fraud statutes.[50] The Coreflood botnet recorded usernames and passwords on infected computers and used them to steal money from the victims' bank accounts.[51] In an "extraordinary intervention,"[52] the United States received an ex parte temporary restraining order, allowing it to seize the botnet command and control servers, replace them with a server run by an Internet hosting provider, and issue a command to infected computers to cease running the malicious software.[53]

More recently, private companies and law enforcement have collaborated on botnet takedowns. In at least some of these collaborative cases, it appears that the impetus for the takedowns came from the private sector, rather than from the government. For example, in June 2013, Microsoft and financial institutions worked with the FBI to disrupt botnets that infected computers with "Citadel" malware and, according to the FBI, caused over $500 million in financial fraud by stealing and using banking credentials.[54] According to reports, "Microsoft and the banks had spied on

47. Cranton, *supra* note 43; *see also* Wingfield & Worthen, *supra* note 44.

48. *R.I.P. Waledac: Undoing the Damage of a Botnet*, MICROSOFT (Sept. 8, 2010), http://blogs.microsoft.com/blog/2010/09/08/r-i-p-waledac-undoing-the-damage-of-a-botnet/ [https://perma.cc/7LMH-7CLZ] (highlighting the issuance of a final judgment in the editor's note).

49. James M. Cole, Deputy Att'y Gen., U.S. Dep't of Justice, Address at the Georgetown Cybersecurity Law Institute (May 23, 2013), https://www.justice.gov/opa/speech/deputy-attorney-general-james-m-cole-addresses-georgetown-cybersecurity-law-institute [https://perma.cc/VEF8-7CKY] (explaining that the Department of Justice "did some creative lawyering to seize control of" the Coreflood botnet command and control servers).

50. Temporary Restraining Order at 1, United States v. John Doe, No. 3:11-cv-00561 (D. Conn. Apr. 12, 2011).

51. Kim Zetter, *With Court Order, FBI Hijacks 'Coreflood' Botnet, Sends Kill Signal*, WIRED (Apr. 13, 2011), http://www.wired.com/2011/04/coreflood/ [https://perma.cc/Q93T-MXY4].

52. *Id.*

53. Temporary Restraining Order, *supra* note 50, at 2–8. For an analysis of the Fourth Amendment implications of the Coreflood takedown, see generally Zeitlin, *supra* note 42.

54. *Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary*, 113th Cong. (2014) (statement of Joseph Demarest, Assistant Director, Cyber Division, Federal Bureau of Investigation), https://www.fbi.gov/news/testimony/taking-down-botnets [https://perma.cc/274Z-6DQF]; *FBI and Microsoft Take Down $500m-Theft Botnet Citadel*, BBC (June 6, 2013), http://www.bbc.com/news/technology-22795074 [https://perma.cc/9864-4SDE].

Citadel for six months before talking to the FBI."[55] After Microsoft reached out to the FBI, federal marshals accompanied Microsoft employees to "two Internet hosting facilities" where "they gathered forensic evidence to attack Citadel's network of botnets."[56] Citadel was the first takedown on which Microsoft "teamed up with the FBI," but it was Microsoft's seventh botnet takedown overall.[57]

Both the companies and the government have publicly embraced their collaboration on botnet takedowns. For example, in December 2013, the FBI, Europol, Microsoft, and other private-industry partners worked together to disrupt the ZeroAccess botnet.[58] A Microsoft press release noted that the takedown "demonstrates the value coordinated operations have against cybercriminal enterprises."[59] FBI Executive Assistant Director Richard McFeely declared that the "disruption of the ZeroAccess botnet is another example of the power of public-private partnerships."[60] In discussing another botnet takedown, Assistant Attorney General Leslie Caldwell explained that the operation's success "was achieved only due to the invaluable technical assistance of Dell SecureWorks and CrowdStrike and help from numerous other companies like Microsoft and Shadowserver."[61] Moreover, she declared that "the sort of collaboration that we achieved in the Gameover Zeus operation was not an aberration. It is the new normal."[62]

As these examples illustrate, the work of pursuing cybercriminals who deploy botnets is done sometimes by the private sector, sometimes by the government, and sometimes by the two acting together.[63] The private sector

---

55. SHANE HARRIS, @WAR, at 119 (2014).

56. *Id.*

57. *Id.*

58. Press Release, Microsoft, Microsoft, the FBI, Europol, and Industry Partners Disrupt the Notorious ZeroAccess Botnet (Dec. 5, 2013), http://news.microsoft.com/2013 /12/05/microsoft-the-fbi-europol-and-industry-partners-disrupt-the-notorious-zeroaccess-botnet/ [https://perma.cc/3BLH-4ZNW]. The botnet generated revenue by, among other things, "search hijacking"—"redirect[ing] people to sites they had not intended or requested to go to in order to steal the money generated by their ad clicks." *Id.*

59. *Id.*

60. *Id.*

61. Leslie R. Caldwell, Assistant Att'y Gen., U.S. Dep't of Justice, Remarks at the Georgetown Cybersecurity Law Institute (May 20, 2015), http://www.justice.gov/opa/speech /assistant-attorney-general-leslie-r-caldwell-delivers-remarks-georgetown-cybersecurity [https://perma.cc/W4XA-9QR8].

62. *Id.*

63. Other companies have begun to engage in takedowns as well. *See, e.g.*, Michael Mimoso, *Facebook Carries Out Lecpetex Botnet Takedown*, THREATPOST (July 9, 2014), http://threatpost .com/facebook-carries-out-lecpetex-botnet-takedown/107096 [https://perma.cc/45FE-7UE9] (describing Facebook's takedown of a botnet operating in Greece that used Facebook "to spread spam and malware"). Takedowns are also not a purely U.S. phenomenon. *See Dutch Team Up with Armenia for Bredolab Botnet Take Down*, N.Y. TIMES (Oct. 26, 2010), http://www.nytimes.com/external/idg/2010/10/26/26idg-dutch-team-up-with-armenia-for-

pioneered the legal tactics underpinning the takedown operations and has continued to drive at least some of the takedowns, like the Citadel operation described above. The "new normal" of public-private collaboration in takedowns preserves a large role for the private sector in setting the agenda for and operationalizing takedown operations.[64]

2. Securing Software.—The roles of the public and private sectors have also blurred, through both collaboration and at least partial role reversals, with respect to securing software. Software flaws or "bugs" are frequent vectors for cybersecurity compromises, and software makers issue patches to fix known bugs.[65] Questions about public and private roles and collaboration arise most often with respect to so-called zero-day exploits. Zero-day vulnerabilities are "exploitable vulnerabilities that a software vendor is not aware of and for which no patch has been created."[66] They are called "zero days" because "the developers or system owners have had zero days to address or patch the vulnerability,"[67] and thus "everyone is vulnerable to exploitation."[68]

Zero-day vulnerabilities are bought and sold in black and gray markets.[69] But the markets are not merely for criminals looking to exploit vulnerabilities. Reports indicate that "governments are increasingly showing up as buyers,"[70] as are companies, like major defense contractors, that act as

---

bredolab-botnet-take-53590.html [https://perma.cc/SM4F-3NDA] [hereinafter *Dutch Team Up*] (describing a takedown operation by Dutch law enforcement).

64. Takedown operations carry a risk of collateral damage, including inadvertent disruption of legitimate websites or interference with the work of security researchers who are tracking the bot herders. *See, e.g.*, Gary Davis, *Microsoft Knocks Botnet, and Four Million Legitimate Users, Offline*, INTEL SECURITY: BLOGS (July 3, 2014), https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/microsoft-knocks-botnet-offline/ [https://perma.cc/6PXU-7VRD].

65. For examples of security updates, see *Apple Security Updates*, APPLE, https://support.apple.com/en-us/HT201222 [https://perma.cc/PLM6-85F3]; *Chrome Releases: Release Updates from the Chrome Team*, GOOGLE, https://googlechromereleases.blogspot.com/ [https://perma.cc/9WWB-BZWV]; *Microsoft Security Bulletins*, MICROSOFT: TECHNET, https://technet.microsoft.com/en-us/security/bulletins [https://perma.cc/28S4-QBZS].

66. LILLIAN ABLON ET AL., NAT'L SECURITY RESEARCH DIV., RAND CORP., MARKETS FOR CYBERCRIME TOOLS AND STOLEN DATA: HACKERS' BAZAAR 25 (2014), http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf [https://perma.cc/JX7T-6VXX].

67. RICHARD A. CLARK ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 219–20 (2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [https://perma.cc/3WGX-YKJN] [hereinafter PRESIDENT'S REVIEW GROUP].

68. ABLON ET AL., *supra* note 66, at 25.

69. For a description of zero-day markets, see *id.* at 25–28.

70. *Id.* at 25; *see also* Nicole Perlroth & David E. Sanger, *Nations Buying as Hackers Sell Flaws in Computer Code*, N.Y. TIMES (July 13, 2013), http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html [https://perma.cc/6HJ2-6FVH]

intermediaries for governments.[71] The "gray market" is "'gray' only because the buyers and sellers are presumed to be the good guys, acting in the interest of public safety and national security," though government purchasers may misuse vulnerabilities or "pass them to another government that will."[72] Shane Harris explains the "gray market" process in his book *@War*:

> [S]ecurity researchers—another term for hackers—find vulnerabilities. . . . The researchers then design exploits, or methods for attacking the vulnerability, that only they know about at this point. Next, they sell the exploits to middlemen, which are mostly large defense contractors. Raytheon and Harris Corporation are two major players in the zero day market. . . . Also collecting and selling zero days are smaller boutique firms, a number of which are run by former military officials or intelligence officials. Once the middlemen have the zero days, they sell them to their customer—the [National Security Agency].[73]

Other companies have built business models selling not just to the U.S. government but also to other companies and governments around the world, including governments with poor human rights records.[74]

The sales prices for zero days vary. A recent RAND Corporation report suggests that the prices "range from a few thousand dollars to $200,000–$300,000, depending on the severity of the vulnerability, complexity of the exploit, how long the vulnerability remains undisclosed, the vendor product involved, and the buyer."[75] Others have suggested that "weaponized" exploits—those that are "ready to use against a system"—"start at around $50,000 and run to more than $100,000 apiece," though prices for exploits targeting particularly valuable or difficult to crack systems may be higher.[76] For example, in 2015, a company paid a million dollars to hackers who

---

(identifying governmental buyers, including, among others, the United States, Israel, the United Kingdom, Russia, India, North Korea, Malaysia, and Singapore).

71. *See* ABLON ET AL., *supra* note 66, at 26 (providing examples of companies that act as intermediaries).

72. KIM ZETTER, COUNTDOWN TO ZERO DAY: STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON 101 (2014); *see also* Jay P. Kesan & Carol M. Hayes, *Bugs in the Market: Creating a Legitimate, Transparent, and Vendor-Focused Market for Software Vulnerabilities*, 58 ARIZ. L. REV. 753, 800–01 (2016) (discussing the white, black, and gray markets for vulnerabilities).

73. HARRIS, *supra* note 55, at 94.

74. *See* Kim Zetter, *Hacking Team Leak Shows How Secretive Zero-Day Exploit Sales Work*, WIRED (July 24, 2015), http://www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work/ [https://perma.cc/FS9M-NAYR] (discussing sales of zero days by some companies to the Italian company, Hacking Team, which "has come under attack for selling to repressive regimes, who've used [Hacking Team products] to target political activists and dissidents").

75. ABLON ET AL., *supra* note 66, at 26.

76. HARRIS, *supra* note 55, at 95–96.

developed an exploit for Apple's iOS,[77] and the U.S. government paid at least $1.3 million for a means of accessing the iPhone used by the perpetrators of the mass shooting in San Bernardino in 2015.[78]

For software vendors, the incentive to patch vulnerabilities in their products is clear. If a vulnerability in a company's software is used for cybercrime or other malicious activity, the company can suffer significant reputational harm.[79] For governments, however, the incentive structure is more complex. On the one hand, zero-day vulnerabilities are valuable tools that allow the government to engage in espionage, but on the other hand, the same vulnerability the government uses offensively presents national security risks if a foreign government discovers and exploits it against, for example, U.S. critical infrastructure.[80] The interests of the software vendors and the U.S. government with respect to discovering and fixing vulnerabilities are not necessarily aligned. The government may want to exploit vulnerabilities that software companies want to fix.[81]

Reports indicate that the National Security Agency (NSA) discovers most of the zero-day vulnerabilities it uses, but it also spends significant money purchasing vulnerabilities.[82] The NSA is "widely believed by security

---

77. *See* Andy Greenberg, *Hackers Claim Million-Dollar Bounty for iOS Zero Day Attack*, WIRED (Nov. 2, 2015), http://www.wired.com/2015/11/hackers-claim-million-dollar-bounty-for-ios-attack/ [https://perma.cc/9XHQ-KLAB] (reporting that "security startup" Zerodium, which had issued a public call for such a vulnerability, paid out the $1 million bounty and would not "immediately report the vulnerabilities to Apple, though it may 'later' tell Apple's engineers the details of the technique to help them develop a patch against the attack").

78. Eric Lichtblau & Katie Benner, *F.B.I. Director Suggests Bill for iPhone Hacking Topped $1.3 Million*, N.Y. TIMES (Apr. 21, 2016), http://www.nytimes.com/2016/04/22/us/politics/fbi-director-suggests-bill-for-iphone-hacking-was-1-3-million.html [https://perma.cc/6GA7-Z2A5].

79. *See, e.g.*, Brian Barrett, *Flash. Must. Die.*, WIRED (July 15, 2015), http://www.wired.com/2015/07/adobe-flash-player-die/ [https://perma.cc/BLK9-W4EP] (chronicling efforts by tech-industry leaders to end use of Adobe Flash after the discovery of numerous zero-day vulnerabilities). Software makers, however, do not suffer legal risk. *See* Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1034 (2014) (explaining that software vendors are "virtually immune for these failures [to secure software], even if the flaw existed due to the company's negligence" because "[e]nd-user license agreements typically disclaim all liability on the vendor's part, and tort law has failed to impose a duty of care on software manufacturers" (footnote omitted)).

80. *Cf.* PRESIDENT'S REVIEW GROUP, *supra* note 67, at 219 (arguing that to assist in protecting privately owned critical infrastructure "NSA, DHS, and other agencies should identify vulnerabilities in software widely employed in critical infrastructure and then work to eliminate those vulnerabilities as quickly as possible," but recognizing that "[t]hat duty to defend, however, may sometimes come into conflict with the intelligence collection mission, particularly when it comes to . . . 'Zero Days'").

81. *See* ZETTER, *supra* note 72, at 221 ("[W]hen military and intelligence agencies need a zero-day vulnerability for offensive operations, the last thing they want to do is have it patched. Instead, they keep fingers crossed that no one else will discover and disclose it before they've finished exploiting it.").

82. *See, e.g.*, *id.* at 219 ("Although most of the implants used by the NSA are designed in-house by the agency's TAO division, the NSA also budgeted $25.1 million in 2013 for 'covert purchases

experts and government officials to be the single largest procurer of zero day exploits," many purchased "in a shadowy online bazaar of freelance hackers and corporate middlemen,"[83] and it has been stockpiling vulnerabilities since the 1990s.[84] The NSA has even paid "software and hardware companies not to disclose vulnerabilities or backdoors in their products, so that the spy agency . . . can exploit them."[85]

In 2014, the U.S. government provided some information on how it decides whether or not to disclose vulnerabilities to software makers so that they can be fixed. In a post on the White House website, Cybersecurity Coordinator Michael Daniel recognized the tradeoffs between using vulnerabilities for intelligence collection and disclosing them so that systems can be secured.[86] In light of this tradeoff, he explained that "*in the majority of cases*, responsibly disclosing a newly discovered vulnerability is clearly in the national interest."[87] But he also set out factors that govern when the government will "temporarily withhold[] knowledge of a vulnerability,"[88]

---

of software vulnerabilities' from private vendors—that is, the boutique firms and large defense contractors who compose the new industrial war complex that feeds the zero-day gray market.").

83. HARRIS, *supra* note 55, at 94.

84. *Id.*

85. *Id.* at 71.

86. Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, WHITE HOUSE (Apr. 28, 2014), https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities [https://perma.cc/K5MZ-Z4DV]; *see also* EFF v. NSA, ODNI – *Vulnerabilities FOIA*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/cases/eff-v-nsa-odni-vulnerabilities-foia [https://perma.cc/5Wg2-CEGH] (collecting government documents on the vulnerability disclosure process released pursuant to a Freedom of Information Act request).

87. Daniel, *supra* note 86 (emphasis added); *see also id.* ("[D]isclosing vulnerabilities *usually* makes sense." (emphasis added)). Reports differ regarding the percentage of vulnerabilities that the U.S. government discloses, as well as whether the government discloses the vulnerabilities only after exploiting them. *See, e.g.*, Chris Strohm et al., *Thank You for Hacking iPhone, Now Tell Apple How You Did It*, BLOOMBERG (Mar. 22, 2016), http://www.bloomberg.com/news /articles/2016-03-23/thank-you-for-hacking-iphone-now-tell-apple-how-you-did-it [https://perma.cc/835S-JYD4] (reporting, based on statements by a "person familiar with the White House's equities review process," that in a single year the government retained "only about two [vulnerabilities] for offensive purposes out of about 100 the White House reviewed"); *Discovering IT Problems, Developing Solutions, Sharing Expertise*, NAT'L SEC. AGENCY (Oct. 30, 2015), https://www.nsa.gov/news-features/news-stories/2015/discovering-solving-sharing-it-solutions.shtml [https://perma.cc/C3NX-FKS4] (reporting that "[h]istorically, NSA has released more than 91 percent of vulnerabilities discovered in products that have gone through [NSA's] internal review process and that are made or used in the United States," while the other "9 percent were either fixed by vendors before [NSA] notified them or not disclosed for national security reasons").

88. Daniel, *supra* note 86 (setting out factors, including the extent to which the "vulnerable system [is] used in the core internet infrastructure, in other critical infrastructure systems, in the U.S. economy, and/or in national security systems," and "[h]ow badly" the United States needs the intelligence it can obtain by using the vulnerability). Daniel's post suggests that the government withholds vulnerabilities in a broader range of circumstances than recommended by the President's Review Group on Intelligence and Communications Technologies. *See* PRESIDENT'S REVIEW

thereby admitting that in fact the U.S. government chooses not to disclose some vulnerabilities of which it is aware.[89]

In an attempt to better secure their software and compete with the vulnerability markets, some companies, particularly in the technology sector,[90] have created "bug bounty" programs through which they pay security researchers (hackers) to disclose vulnerabilities to the software company so that the vulnerabilities can be patched.[91] Google, for example, paid out more than $2 million in bounties in 2015.[92] However, the companies have difficulty competing with the black and gray markets, where "a researcher could earn 10–100 times what a software vendor with a bug bounty would pay."[93] Moreover, some reports indicate that governments

---

GROUP, *supra* note 67, at 219 ("In rare instances, [U.S.] policy may briefly authorize using a Zero Day for high priority intelligence collection, following senior, interagency review involving all appropriate departments."); Jack Goldsmith, *Thoughts on the White House Statement on Cyber Vulnerabilities*, LAWFARE (Apr. 28, 2014), http://www.lawfareblog.com/thoughts-white-house-statement-cyber-vulnerabilities [https://perma.cc/A987-LW54] (suggesting that Daniel's post "implies that the government will store and possibly use vulnerabilities . . . in a wider array of circumstances than" the President's Review Group recommended).

89. ZETTER, *supra* note 72, at 391–92 (discussing "loopholes" in the U.S. government's vulnerability disclosure policy).

90. Technology companies' bug bounty programs are the exception, not the rule, among major companies. According to a recent study, 94% of companies included in the Forbes Global 2000 "did not advertise a way for so-called ethical hackers to report bugs," much less pay hackers to report them. Danny Yadron, *If You Find a Software Bug, Don't Try to Report It to These Companies*, WALL STREET J. (Nov. 5, 2015), http://blogs.wsj.com/digits/2015/11/05/if-you-find-a-software-bug-dont-try-to-report-it-to-these-companies/ [https://perma.cc/N5LD-PNCJ].

91. *See, e.g.*, *Chrome Reward Program Rules*, GOOGLE, https://www.google.com/about/appsecurity/chrome-rewards/index.html [https://perma.cc/L92G-EDVJ]; *Information*, FACEBOOK, https://www.facebook.com/whitehat/bounty/ [https://perma.cc/26UF-GXUQ]; *see also* Nicole Perlroth, *HackerOne Connects Hackers With Companies, and Hopes for a Win-Win*, N.Y. TIMES (June 7, 2015), http://www.nytimes.com/2015/06/08/technology/hackerone-connects-hackers-with-companies-and-hopes-for-a-win-win.html [https://perma.cc/NN7T-NP6X] (profiling HackerOne, a company that interfaces between companies and white-hat hackers and handles bug bounty payouts in exchange for a percentage of the bounty). For lists of companies that have bounty programs, see, for example, *The Bug Bounty List*, BUGCROWD, https://bugcrowd.com/list-of-bug-bounty-programs [https://perma.cc/9BKQ-JYES]; *Bug Bounties & Disclosure Programs*, BUGSHEET, http://bugsheet.com/directory [https://perma.cc/WNA2-L57B].

92. Eduardo Vela Nava, *Google Security Rewards – 2015 Year in Review*, GOOGLE SECURITY BLOG (Jan. 28, 2016), https://security.googleblog.com/2016/01/google-security-rewards-2015-year-in.html [https://perma.cc/H8GG-NH9G]; *see also* Reginaldo Silva, *2015 Highlights: Less Low-Hanging Fruit*, FACEBOOK (Feb. 9, 2016), https://www.facebook.com/notes/facebook-bug-bounty/2015-highlights-less-low-hanging-fruit/1225168744164016 [https://perma.cc/9WBN-UP5B] (noting that Facebook paid out $936,000 in bounties in 2015). For an overview of the current bug bounty market, see BUGCROWD, THE STATE OF BUG BOUNTY (2016), https://pages.bugcrowd.com/hubfs/PDFs/state-of-bug-bounty-2016.pdf [https://perma.cc/F4PZ-7WWC].

93. ABLON ET AL., *supra* note 66, at 26; *see* ZETTER, *supra* note 72, at 102–03 (explaining that bug bounty programs are "still no match, in most cases, for the price some governments will pay on the gray market").

have driven up market prices, making it more difficult for companies to compete.[94]

The recent fight between Apple and the FBI over access to the San Bernardino shooter's iPhone provides a dramatic example of an adversarial relationship between the private sector and the government over software security. In February 2016, the Department of Justice obtained a court order compelling Apple to assist the government in accessing the shooter's iPhone by writing code to disable security features, including a setting that would erase the data on the phone after entry of erroneous passcodes.[95] Apple challenged the order,[96] and on the eve of a hearing, the government revealed that a third party had provided a way for the government to access the iPhone without Apple's assistance.[97] The government has subsequently indicated that it paid an outside party over $1.3 million for a tool to access the iPhone.[98] The FBI rejected calls to disclose the iPhone vulnerability for patching and instead declared that the FBI would not even submit the access tool's underlying vulnerability to the "vulnerability equities process" because the government did not "purchase the rights to technical details about how the method functions, or the nature and extent of any vulnerability upon which the method may rely in order to operate."[99] This incident raises the specter not only of the government strategically manipulating what exactly it acquires and thus what enters the vulnerability equities process but also of private hackers potentially limiting the government's options by imposing contractual nondisclosure obligations as part of the government's purchase of hacking tools.

---

94. *See* HARRIS, *supra* note 55, at 102 (reporting Google employees' statements that the company's "biggest competition on the zero day gray market is the NSA," which is "buying up zero days faster than anyone else, and paying top dollar"); Joseph Menn, *Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback*, REUTERS (May 10, 2013), http://www.reuters.com/article/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510 [https://perma.cc/6LZM-G9WQ] (noting that the U.S. government is the "biggest buyer in a burgeoning gray market" for zero-day vulnerabilities).

95. In the Matter of the Search of an Apple Iphone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. ED 15-0451M, 2016 WL 618401, at *2 (C.D. Cal. Feb. 16, 2016).

96. Apple, Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Apple's Assistance at 2, In the Matter of the Search of an Apple Iphone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. CM 16-10 (C.D. Cal. Feb. 25, 2016).

97. Government's *Ex Parte* Application for a Continuance at 3, In the Matter of the Search of an Apple Iphone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. CM 16-10 (C.D. Cal. Mar. 21, 2016).

98. *See supra* note 78 and accompanying text.

99. Eric Tucker, *FBI Says It Won't Disclose How It Accessed Locked iPhone*, ASSOCIATED PRESS (Apr. 27, 2016), http://bigstory.ap.org/article/3ed26fcb4eb0453ea8de7f0cbbebf2bc/fbi-says-it-wont-disclose-how-it-accessed-locked-iphone [https://perma.cc/8AD5-EAEJ] (quoting a statement by FBI official Amy Hess).

On the other hand, more recently, the Defense Department has taken a page from the private sector's playbook and established a bug bounty program of its own—a first for the federal government.[100] Called "Hack the Pentagon," the program allowed white-hat hackers—after registering and completing a background check—to submit vulnerabilities in the Department's public-facing websites, like defense.gov.[101] The Defense Department ultimately paid out $150,000 for more than 100 vulnerabilities.[102]

As these examples make clear, the relationship between the government and the private sector with respect to vulnerabilities is complex. Sometimes the government partners with the private sector to secure companies' software, such as when the government purchases and discloses a vulnerability to the software vendor so the vendor can patch it. Sometimes the government seeks nongovernmental help to secure *the government's* systems and networks, as in the Defense Department bug bounty program. On other occasions, the government and the private sector reportedly partner *not* to secure software, such as when the NSA pays companies not to fix software vulnerabilities,[103] presumably in the service of broader intelligence and national security goals. But the picture is not all rosy: sometimes the government and software companies are adversaries. This occurs when the government discovers and fails to disclose a vulnerability that the software company would otherwise fix; when the government exploits a vulnerability in a company's product; or when the government purchases a vulnerability in a company's software on the gray market (and fails to disclose it).[104] In

100. Press Release, U.S. Dep't of Def., Statement by Pentagon Press Secretary Peter Cook on DoD's "Hack the Pentagon" Cybersecurity Initiative, U.S. Dep't of Defense (Mar. 2, 2016), http://www.defense.gov/News/News-Releases/News-Release-View/Article/684106/statement-by-pentagon-press-secretary-peter-cook-on-dods-hack-the-pentagon-cybe [https://perma.cc/X76B-BVHA].

101. *Id.*; Lisa Ferdinando, *Carter Announces 'Hack the Pentagon' Program Results*, DOD NEWS (June 17, 2016), http://www.defense.gov/News/Article/Article/802828/carter-announces-hack-the-pentagon-program-results [https://perma.cc/AP9V-3HCT].

102. Ferdinando, *supra* note 101. Although the "Hack the Pentagon" program was time-limited, the Defense Department recently announced a separate "Vulnerability Disclosure Policy" that is designed to allow researchers to report vulnerabilities to the Defense Department without fear of criminal prosecution or civil lawsuits. *DoD Vulnerability Disclosure Policy*, HACKERONE, https://hackerone.com/deptofdefense [https://perma.cc/652R-69ZF]; Ellen Nakashima, *Hackers Can Now Report Bugs in Defense Dept. Websites Without Fear of Prosecution*, WASH. POST (Nov. 21, 2016), https://www.washingtonpost.com/world/national-security/hackers-can-now-report-bugs-in-defense-dept-websites-without-fear-of-prosecution/2016/11/21/2605901a-b019-11e6-840f-e3ebab6bcdd3_story.html?utm_term=.89964c35e148 [https://perma.cc/Y5ZX-7S62].

103. HARRIS, *supra* note 55, at 71 ("[T]he NSA pays software and hardware companies not to disclose vulnerabilities or backdoors in their products, so that the spy agency and TAO hackers can exploit them.").

104. The plasticity of roles is also evident for those who discover vulnerabilities. *See* WITTES & BLUM, *supra* note 2, at 86 ("Those who look for and discover zero-day flaws can thus function

these latter situations, the software companies that seek to secure their software (where the government does not) are arguably acting in a government-like fashion: they are trying to protect individual, corporate, and other systems against cybercrime and other exploitation. At the same time, the government acts as a participant in the zero-day market, rather than a regulator,[105] potentially sacrificing individual-level security (what the software makers aim to address) in the service of broader national security goals.

3. Publicly Attributing State-Sponsored Intrusions.—For the last several years, private companies have begun to publicly accuse foreign governments and government-sponsored actors of hacking targets in the United States and elsewhere. In notable instances like the 2015 hack of the Office of Personnel Management (OPM)[106] and the recent breaches of the Democratic National Committee,[107] private cybersecurity companies have taken the lead in public attribution of hacks to foreign governments when the U.S. government was reluctant to make similar accusations.

This phenomenon of private attribution of state-sponsored hacking has created an informal, but mutually beneficial, partnership between the cybersecurity companies and the U.S. government. On the one hand, the companies use public attribution reports for marketing purposes and to generate business. On the other hand, the government uses the reports to talk around classified information and to distance itself from accusations.[108]

---

as outlaws (if they mean to exploit them for criminal purposes), as a crucial line of defense (if they mean to help software vendors secure them before an attack), or as a component of aggressive state or nonstate offense (if they mean to help attack someone else).").

105. The U.S. government may begin regulating some cross-border aspects of trade in hacking-related software pursuant to the Wassenaar Arrangement. Changes to the Arrangement in 2013 required countries to regulate cross-border trade in "intrusion software," but after protests from the technology and cybersecurity communities, the White House announced in March 2016 that it would attempt to renegotiate the 2013 changes. Sean Gallagher, *US to Renegotiate Rules on Exporting "Intrusion Software,"* ARS TECHNICA (Mar. 2, 2016), http://arstechnica.com/tech-policy/2016/03/us-to-renegotiate-rules-on-exporting-intrusion-software-under-wassenaar-arrangement/ [https://perma.cc/2BCG-64S9]. That effort largely failed in December 2016, *see* Tami Abdollah, *US Fails to Renegotiate Arms Control Rule for Hacking Tools*, ASSOCIATED PRESS (Dec. 19, 2016), http://bigstory.ap.org/article/c0e437b2e24c4b68bb7063f03ce892b5/us-fails-renegotiate-arms-control-rule-hacking-tools [https://perma.cc/8JM8-EPSZ], and it is not clear whether the Trump Administration will renew efforts to renegotiate the 2013 requirements.

106. *See infra* note 120 and accompanying text.

107. *See infra* notes 288–89 and accompanying text.

108. For example, in January 2010, Google publicly announced that it had discovered a sophisticated attack on its systems that originated in China. David Drummond, *A New Approach to China*, GOOGLE (Jan. 12, 2010), http://googleblog.blogspot.com/2010/01/new-approach-to-china.html [https://perma.cc/AJQ9-U8BJ]. After the post, then-Secretary of State Hillary Clinton issued a statement that "look[ed] to the Chinese government for an explanation." Hillary Rodham Clinton, U.S. Sec'y of State, U.S. Dep't of State, Statement on Google Operations in China (Jan. 12, 2010), http://www.state.gov/secretary/20092013clinton/rm/2010/01/135105.htm

Several examples illustrate the mutually beneficial relationship that companies and the U.S. government have developed.

In an extensive report published in February 2013, the cybersecurity firm Mandiant described the evidence it had amassed against a group, designated Advanced Persistent Threat 1 (APT1), that had compromised 141 companies in seven years.[109] Mandiant traced the attacks to a particular building in Shanghai and concluded that APT1 is Unit 61398 of the Chinese People's Liberation Army.[110] Based on its research, Mandiant alleged that "the Communist Party of China . . . is tasking the Chinese People's Liberation Army . . . to commit systematic cyber espionage and data theft against organizations around the world."[111] The report provided not only information about APT1's methods of attack, but also details and photos of several "APT1 personas" who "made poor operational security choices" that allowed Mandiant to identify them.[112]

Mandiant apparently coordinated in some manner with the U.S. government before releasing its report.[113] According to subsequent reports, "[s]ources close to the drafting of the report say that the government . . . gave Mandiant some intelligence it used in the report,"[114] and the Department of Homeland Security may have waited until Mandiant's announcement to issue a security bulletin that included some of the same Internet addresses and websites that Mandiant identified.[115]

The Mandiant report triggered a sea change in U.S. policy toward China on cybersecurity issues. It prompted the Obama administration to begin openly calling out the Chinese government for intellectual property theft. Less than a month after the report's release, National Security Advisor Tom Donilon gave a speech to The Asia Society and called on the Chinese government to "take serious steps to investigate and put a stop to these activities."[116] The Mandiant report provided a way for the U.S. government

---

[https://perma.cc/8PKL-Y4XA]. In a later interview, former Deputy Secretary of State Jim Steinberg explained the utility to the government of Google's post, noting that it gave the government "'an opportunity to discuss the issues without having to rely on classified sources or sensitive methods' of intelligence gathering." HARRIS, *supra* note 55, at 174 (quoting Harris's interview with Steinberg).

109. MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 20 (2013), https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf [https://perma.cc/58QK-2JJ5].

110. *Id.* at 3.

111. *Id.* at 7.

112. *Id.* at 51–58.

113. HARRIS, *supra* note 55, at 207.

114. *Id.* at 209.

115. *Id.*

116. Tom Donilon, Nat'l Sec. Advisor, Exec. Office of the President, The United States and the Asia-Pacific in 2013 (Mar. 11, 2013), https://www.whitehouse.gov/the-pressoffice/2013/03/11/remarks-tom-donilon-national-security-advisor-president-united-states-an

to address Chinese cyber intrusions without revealing classified intelligence information or making the accusation itself.[117]

The Mandiant APT1 report started a trend of companies attributing intrusions to governments.[118] And the U.S. government has taken notice. In an April 2015 speech, Secretary of Defense Ash Carter explained that attribution of cyber attacks has improved "because of private-sector security researchers like FireEye, CrowdStrike, HP—when they out a group of malicious cyber attackers, we take notice and share that information."[119]

Carter's statement may undersell the utility of private attribution to the government. A strikingly direct example of outsourcing attribution occurred with the Office of Personnel Management hack. The U.S. government has declined to identify the perpetrators of the intrusions, but cybersecurity firm CrowdStrike—based in part on "technical information provided by the U.S. government" to the company—has alleged that the "intruders were affiliated with the Chinese government."[120]

[https://perma.cc/232W-UXJB]; *see* FRED KAPLAN, DARK TERRITORY: THE SECRET HISTORY OF CYBER WAR 221 (2016) (noting that Donilon's comments on China "broke new diplomatic ground").

117. HARRIS, *supra* note 55, at 208–09 (noting that "Obama administration officials were generally pleased with Mandiant's decision" to issue the report for this reason).

118. Companies, including FireEye, which acquired Mandiant in 2014, and CrowdStrike, have issued numerous reports accusing both the Chinese and Russian governments of intrusions. *See, e.g.*, CROWDSTRIKE, CROWDSTRIKE INTELLIGENCE REPORT: PUTTER PANDA 5 (2014), https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda .original.pdf [https://perma.cc/M7HD-M82H] (accusing Chinese People's Liberation Army (PLA) Unit 61486 of intrusions aimed at, *inter alia*, space and communications); FIREEYE, APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS? 28 (2014), https://www2.fireeye.com/apt28.html [https://perma.cc/F4Q7-Q99T] (alleging that APT28 is "sponsored by the Russian government"); Dmitri Alperovitch, *Bears in the Midst: Intrusion into the Democratic National Committee*, CROWDSTRIKE BLOG (June 15, 2016), https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/ [https: //perma.cc/B7LU-68NJ] (revealing that two groups linked to Russian intelligence agencies compromised the Democratic National Committee). Another category of private sector attributions to state-sponsored actors involves companies providing notices to their customers when they believe the customers' accounts have been targeted by state-sponsored actors. Google pioneered such notifications in 2012, and in late 2015, Facebook, Twitter, Yahoo, and Microsoft followed suit. *See* Kristen Eichensehr, *"Your Account May Have Been Targeted by State-Sponsored Actors": Attribution and Evidence of State-Sponsored Cyberattacks*, JUST SECURITY (Jan. 11, 2016, 9:17 AM), https://www.justsecurity.org/28731/your-account-targeted-state-sponsored-actors-attribution-evidence-state-sponsored-cyberattacks/ [https://perma.cc/D6MW-PVVG] (discussing state-sponsored-attacker notifications and their implications for evolving standards of evidence regarding attribution).

119. Ash Carter, Sec'y of Def., U.S. Dep't of Def., Drell Lecture: Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity (Apr. 23, 2015), http://www.defense.gov /Speeches/Speech.aspx?SpeechID=1935 [https://perma.cc/86HM-AV5M].

120. Shane Harris, *Security Firm: China Is Behind the OPM Hack*, DAILY BEAST (July 9, 2015), http://www.thedailybeast.com/articles/2015/07/09/security-firm-china-is-behind-the-opm-hack.html [https://perma.cc/MAF3-3HTK].

In other instances, companies' independent actions have proven beneficial to government goals. For example, in September 2015, the United States and China agreed that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[121] Commentators immediately questioned how the United States would verify China's compliance with the agreement.[122] Cybersecurity companies were quick to volunteer that they would assist, through their work in monitoring their clients' networks, in verifying China's compliance with the deal.[123]

Despite the U.S. government's apparent enthusiasm for private attribution by U.S. companies, U.S. cybersecurity firms are not the only ones in the attribution business.[124] The United States has been on the receiving

---

121. Office of the Press Sec'y, *Fact Sheet: President Xi Jinping's State Visit to the United States*, WHITE HOUSE (Sept. 25, 2015), https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states [https://perma.cc/Q3KQ-H6ME].

122. *See, e.g.*, *The Obama-Xi Cyber Mirage: A Digital Arms Deal that Is Full of Promises but No Enforcement*, WALL STREET J. (Sept. 27, 2015), http://www.wsj.com/articles/the-obama-xi-cyber-mirage-1443387248 [https://perma.cc/2VBA-AQJJ]; Benjamin Wittes, *China's Cyber-Commitments and Congressional Oversight: A Suggestion*, LAWFARE (Sept. 28, 2015), https://lawfareblog.com/chinas-cyber-commitments-and-congressional-oversight-suggestion [https://perma.cc/Q8C2-ZKJK].

123. *See* Dmitri Alperovitch, *U.S.-China Agreement on Cyber Intrusions: An Inflection Point*, CROWDSTRIKE BLOG (Sept. 25, 2015), http://blog.crowdstrike.com/cyber-agreement/ [https://perma.cc/7NGR-BL2S] (discussing "how [the] private sector can be of help" in "validating this agreement" and noting that CrowdStrike's products will provide "visibility into whether China abides by the commitment[s]" expressed in the agreement); Richard Bejtlich, *To Hack, or Not to Hack?*, BROOKINGS UP FRONT (Sept. 28, 2015), http://www.brookings.edu/blogs/up-front/posts/2015/09/28-us-china-hacking-agreement-bejtlich [https://perma.cc/L3DZ-4CD8] ("I . . . expect U.S. private sector security companies to bear the brunt of the public verification process. They will be subjected to repeated questions such as 'are the Chinese still hacking?' while the U.S. administration is likely to remain fairly quiet."); Kristen Eichensehr, *The US-China Cyber Agreement: What's In and What's Out*, JUST SECURITY (Sept. 28, 2015, 10:10 AM), https://www.justsecurity.org/26412/u-s-china-cyber-agreement-whats-whats/ [https://perma.cc/QL8C-9TYE] (discussing the role of private cybersecurity firms in verification of the intellectual property theft provision). At least one company was also quick to accuse China of noncompliance. *See* Paul Mozur, *Cybersecurity Firm Says Chinese Hackers Keep Attacking U.S. Companies*, N.Y. TIMES (Oct. 19, 2015), http://www.nytimes.com/2015/10/20/technology/cybersecurity-firm-says-chinese-hackers-keep-attacking-us-companies.html [https://perma.cc/JYS9-X2R9] (reporting on allegations by CrowdStrike that actors affiliated with the Chinese government attempted to hack U.S. commercial targets in the wake of the U.S.–China cybersecurity deal).

124. One prominent foreign cybersecurity firm is Russian company Kaspersky Lab, whose founder Eugene Kaspersky "studied cryptography at a high school co-sponsored by the K.G.B. and once worked for the Russian military." Nicole Perlroth & David E. Sanger, *U.S. Embedded Spyware Overseas, Report Claims*, N.Y. TIMES (Feb. 16, 2015), http://www.nytimes.com/2015/02/17/technology/spyware-embedded-by-us-in-foreign-networks-security-firm-says.html [https://perma.cc/9U3H-GL4F]. Kaspersky Lab has been said to have "a front-row seat to America's digital espionage operations" because its security software "is not used by many

end of private attribution, though not to the same extent as other countries.[125] The government connections of cybersecurity-firm personnel, both in the United States and abroad, have prompted controversy[126] and charges of pulling punches for national governments.[127] Cybersecurity companies generally deny such allegations,[128] but FireEye CEO David DeWalt has "said he would think twice before publicizing a . . . hacking campaign by Americans" like the campaigns that FireEye has attributed to states like China and Iran.[129] Such nationalism in the cybersecurity market raises interesting dilemmas for governments and companies, but it also suggests that even if a company is not willing to call out its national government, some other company from abroad might. This may become increasingly likely as new companies enter the attribution business. For example, in May 2015, a Chinese company entered the field. Chinese Internet security company Qihoo 360 released a report on a state-based hacking group, "OceanLotus," though the report did not identify the country responsible.[130]

The private attribution of government attacks is a striking development. Mandiant, CrowdStrike, and the other companies that have accused foreign

---

American government agencies" and is therefore "more trusted by other governments, like those of Iran and Russia, whose systems are closely watched by United States intelligence agencies." *Id.*; *see* WITTES & BLUM, *supra* note 2, at 73–74 (citing Kaspersky Lab as an example and arguing that "[t]he [U.S.] intelligence community is not the only official body seeking the assistance of the private sector").

125. *See, e.g.*, Kim Zetter, *Suite of Sophisticated Nation-State Attack Tools Found with Connection to Stuxnet*, WIRED (Feb. 16, 2015), http://www.wired.com/2015/02/kapersky-discovers-equation-group [https://perma.cc/9B8P-44ZG] (detailing a report by Kaspersky Lab on "Equation Group").

126. *See, e.g.*, Stephanie Mlot, *Kaspersky, Bloomberg Spar over KGB Allegations*, PC MAG. (Mar. 23, 2015), http://www.pcmag.com/article2/0,2817,2478613,00.asp [https://perma.cc/B9PX-JY2Q]; *see also* Corey Flintoff, *Kaspersky Lab: Based in Russia, Doing Cybersecurity in the West*, NPR (Aug. 10, 2015, 1:59 PM), http://www.npr.org/sections/alltechconsidered/2015/08/10/431247980/kaspersky-lab-a-cybersecurity-leader-with-ties-to-russian-govt [https://perma.cc/32TU-KEWC] (noting controversy over Kaspersky's ties to Russian intelligence officials); Danny Yadron, *Cybersecurity Firm's Strategy Raises Eyebrows: FireEye's Plan to Reverse Losses Includes Getting Close to Federal Agencies*, WALL STREET J. (Sept. 8, 2015), http://www.wsj.com/articles/cybersecurity-firms-strategy-raises-eyebrows-1441766359 [https://perma.cc/8QVG-MTNU] (noting that U.S. cybersecurity companies "increasingly stake their reputations on ties to Washington").

127. Danny Yadron, *When Cybersecurity Meets Geopolitics*, WALL STREET J. (Mar. 23, 2015), http://blogs.wsj.com/digits/2015/03/23/when-cybersecurity-meets-geopolitics [https://perma.cc/4CAT-38GZ].

128. *See, e.g.*, Flintoff, *supra* note 126 (citing Kaspersky's denial that it avoids going after "Russian viruses" and instead targets "malware it says comes from Western governments").

129. Yadron, *supra* note 127.

130. *See* Adam Segal, *OceanLotus: China Hits Back With Its Own Cybersecurity Report*, NET POLITICS (June 3, 2015), http://blogs.cfr.org/cyber/2015/06/03/oceanlotus-china-fights-back-with-its-own-cybersecurity-report/ [https://perma.cc/RVE5-3A3Y]; *see also id.* ("Qihoo clearly is co-opting the language and techniques of the APT reports done by Mandiant, CrowdStrike, and other U.S. cybersecurity companies.").

governments of intrusions are engaged in private intelligence-gathering at a sophisticated level.[131] They are in many ways doing what one would expect intelligence agencies to do, but they make their research public and use it to build business.[132] U.S. companies may coordinate in some way with the U.S. government before releasing a report,[133] but it appears that the companies are generally in the driver's seat, deciding which clients to take on, which hackers to investigate, whether to build a case against foreign governments, and whether and when to publicly accuse foreign states of wrongdoing. Although the U.S. government appears to have appreciated and even benefited from Mandiant's release of its APT1 report, the report "set off a bomb in one of the most delicate and thorny areas of [U.S.] foreign policy."[134] And the decision to launch the bomb came from a private company marketing its services,[135] not from the government agencies charged with diplomacy, national defense, or intelligence.

The U.S. government, in line with Carter's speech, has encouraged the attribution of state-sponsored attacks and fostered an informal partnership of sorts with cybersecurity companies. But this may be a tenuous and even dangerous alliance. It is not clear that the incentives of U.S. companies, which have commercial reasons for attributing state-sponsored hacks, will always align with the public values the U.S. government is supposed to serve.[136]

4. Defending Private Networks.—Private parties own roughly 85% of the critical infrastructure in the United States,[137] and the issue of who should

131. Kristen Eichensehr, *The Private Frontline in Cybersecurity Offense and Defense*, JUST SECURITY (Oct. 30, 2014, 12:37 PM), http://justsecurity.org/16907/private-frontline-cybersecurity-offense-defense/ [https://perma.cc/DB4V-DL8A]; *see also* WITTES & BLUM, *supra* note 2, at 69–70 (noting that the Mandiant APT1 report takes "DIY signals counterintelligence to a whole new level").

132. HARRIS, *supra* note 55, at 206 ("The details in the Mandiant report were of a kind one normally expects to find in a classified government intelligence document. . . . The report showed that private investigators could collect and analyze information as effectively as a government spy agency, if not more so."); SEGAL, *supra* note 9, at 8 (noting with respect to Mandiant's APT1 report that "[i]n attributing the digital assault, a private company had acted like a national intelligence agency").

133. *See, e.g.*, Yadron, *supra* note 127 ("Before American computer-security company FireEye releases a report on new hacker activity, it sometimes gives the U.S. government an advance copy.").

134. HARRIS, *supra* note 55, at 205.

135. *See* KAPLAN, *supra* note 116, at 223 (reporting that Mandiant gave *The New York Times* an advance copy of the APT1 report, and "[t]he *Times* ran a long front-page story summarizing its contents"); *see also infra* note 174.

136. On the other hand, if the U.S. government ceases making public attributions, private companies' attribution reports may play an increasingly important role. *See infra* note 308.

137. *Critical Infrastructure and Key Resources*, INFO. SHARING ENV'T, http://www.ise.gov/mission-partner/critical-infrastructure-and-key-resources [https://perma.cc/D9JX-D4LT]; *cf.*

defend such networks from cybersecurity threats has provoked uncertainty and disagreement.[138] Is securing critical infrastructure networks a public good that should be provided by the government, like traditional national defense,[139] or is it the responsibility of individual companies?[140] In the last few years, the federal government and the private sector have exhibited contradictory views about who should defend the networks, and their views contradict not just each other but their own positions over time.

In some circumstances, the private sector has wanted the federal government to provide defense. For example, after Google was hacked by China in 2010, a "former White House official" recounted to a journalist that Google "called the N.S.A. in and said, 'You were supposed to protect us from this!' The N.S.A. guys just about fell out of their chairs. They could not believe how naïve the Google guys had been."[141]

More recently, however, the NSA has reportedly sought greater access to private networks to provide defense and has been rebuffed. Shane Harris recounts a 2011 meeting between then-NSA director Keith Alexander and financial industry leaders. Alexander told the executives that the NSA wanted to expand to banks a pilot program, whereby the NSA had been sharing cyber threat indicators with defense contractors, but "this time with a twist."[142] Alexander suggested that

> [it] would be much easier to protect the companies . . . if they let the NSA install surveillance equipment on their networks. Cut out the

---

Carter, *supra* note 119 ("American businesses own, operate, and see approximately ninety percent of our national networks . . . .").

138. *See* Robert Knake, *Private Sector and Government Collaboration on Cybersecurity: The Home Depot Model*, COUNCIL ON FOREIGN REL.: NET POLITICS (Mar. 31, 2015), http://blogs.cfr.org/cyber/2015/03/31/private-sector-and-government-collaboration-on-cybersecurity-the-home-depot-model/ [https://perma.cc/9B9D-DGF9] (noting continued uncertainty among companies' chief information security officers about the relative roles of the government and private sector in addressing cybersecurity incidents).

139. *See, e.g.*, Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1518 (2013) (suggesting that "private firms might be asked to provide a baseline level of cyber-security . . . defenses that are capable of thwarting intrusions by adversaries of low to medium sophistication" while the government "assume[s] responsibility for defending public utilities and other sensitive enterprises against catastrophic attacks by foreign militaries and other highly sophisticated adversaries"); Alan Charles Raul, *Cyberdefense Is a Government Responsibility*, WALL STREET J. (Jan. 5, 2015), http://www.wsj.com/articles/alan-charles-raul-cyberdefense-is-a-government-responsibility-1420502942 [https://perma.cc/TP3Q-PD6W].

140. *See* Madeline Carr, *Public–Private Partnerships in National Cyber-Security Strategies*, 92 INT'L AFF. 43, 56–57 (2016) (discussing the divergent perspectives of governments and private actors regarding whether protecting private networks is a "public good" and should be the government's responsibility).

141. Michael Joseph Gross, *Enter the Cyber-Dragon*, VANITY FAIR (Aug. 2, 2011), http://www.vanityfair.com/news/2011/09/chinese-hacking-201109 [https://perma.cc/9CZY-UL4K].

142. HARRIS, *supra* note 55, at 166.

> middlemen. Let the analysts at Fort Meade have a direct line into Wall Street.
>
> A silence fell over the room. The executives looked at one another, incredulous. *Is this guy serious?*
>
> "They thought he was an idiot," says a senior financial services executive who was at the meeting . . . . "These are all private networks he was talking about."[143]

The ramifications for companies of allowing direct NSA access to their networks are even greater in the wake of the Snowden revelations, as a result of which "[t]here is now business value in championing privacy and fighting the NSA, and business harm in cooperation."[144]

The basic system that has evolved for securing critical infrastructure systems from cybersecurity breaches casts the private sector as the main actor—either companies defend their own networks, or they hire other companies to do so—and the government plays only a supporting role. As Robert Knake, the former National Security Council director for cybersecurity policy, pithily deemed it, the current system (at least from the government's perspective) is "the 'Home Depot' model: You can do it; we can help!"[145] In other words, "the current strategy makes private companies responsible for their own network defense," while the federal government supports them by "doing the things that only the federal government can do," including prosecuting cybercrime, applying diplomatic pressure, issuing sanctions, providing cyber-threat information to companies, and "[d]efend[ing] the United States from significant, national events."[146]

---

143. *Id.* This was not the first time that government officials had considered—or the NSA had suggested—putting the NSA in charge of securing critical infrastructure computers. *See* KAPLAN, *supra* note 116, at 19–20, 34 (recounting an incident in the Reagan administration); *id.* at 57, 72 (reporting statements then-NSA director Kenneth Minihan made in 1997 to a presidential commission on critical infrastructure protection in which he appeared to suggest the NSA take over cybersecurity for critical infrastructure, stating, in particular, "[c]hange the law, give me the power, I'll protect the nation."); *cf. id.* at 100–01 (noting that an early draft of President Clinton's "*National Plan for Information Systems Protection: Defending America's Cyberspace* . . . proposed hooking up all civilian government agencies—and perhaps, eventually critical infrastructure companies—to a Federal Intrusion Detection Network . . . a parallel Internet, with sensors wired to some government agency's monitor (which agency was left unclear)," though protests from Congress and civil liberties groups ultimately prompted revisions).

144. BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 207 (2015); *see also* Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J. 317, 351 & n.188 (2015) (discussing harms U.S. businesses suffered internationally in the wake of the Snowden revelations).

145. Knake, *supra* note 138. The private sector's take on the model may be somewhat different. Knake notes that a chief information security officer he spoke with "summed up the approach as 'private sector, drop dead.'" *Id.*; *Robert K. Knake*, COUNCIL ON FOREIGN REL., http://www.cfr.org/experts/cybersecurity-homeland-security-digital-infrastructure/robert-k-knake/b15502 [https://perma.cc/6A57-AK89].

146. Knake, *supra* note 138.

Cyber-threat information sharing is the dominant example of partnership between the government and the private sector on cybersecurity.[147] In 2011, the Defense Department launched a pilot program to provide classified, cybersecurity-threat information to a few defense industrial-base companies, and the program has subsequently expanded.[148] The FBI has undertaken similar information sharing with a broader range of industries.[149] For example, the FBI "has broken in to the computers of Chinese hackers and stolen the lists of specific companies they're targeting," as well as "the e-mail addresses of employees whom Chinese hackers intend to spear phish, sending them legitimate-looking e-mails that actually contain spyware."[150] The FBI then provides the information directly to the targeted companies for use in the companies' defensive measures.[151] More recently, the Department of Homeland Security has also begun sharing classified threat information with prequalified private sector entities.[152]

The private sector has come a long way since the Google executives asked why the NSA had failed to protect the company, and private, defensive capacities have strengthened so much that the importance of the government's role in companies' defense is now less clear. In one instance, for example, the FBI shared with banks "the rundown of cases it was tracking, so the banks could see for themselves the breadth of the bureau's knowledge," but "[i]t turned out that the banks had been tracking every case on the list, except one," even without the government's assistance.[153]

---

147. Information sharing is not treated as a separate case study here because it is not an end in itself but rather a means of securing both governmental and private sector networks.

148. For the initial incarnation of the program, see David Ignatius, Opinion, *Department of Internet Defense*, WASH. POST (Aug. 12, 2011), https://www.washingtonpost.com/opinions/department-of-internet-defense/2011/08/12/gIQAPQcxBJ_story.html [https://perma.cc/NBR6-VGD9] (describing the Defense Industrial Base, or "DIB," Cyber Pilot program); Ellen Nakashima, *Cyber Defense Effort Is Mixed, Study Finds*, WASH. POST (Jan. 12, 2012), https://www.washingtonpost.com/world/national-security/cyber-defense-effort-is-mixed-study-finds/2012/01/11/gIQAAu0YtP_story.html [https://perma.cc/7ED8-WJV6] (discussing early evaluations of the DIB Cyber Pilot program). For the current program, see 32 C.F.R. §§ 236.1–236.7 (2016) (outlining the purpose of and requirements for the DoD–DIB cybersecurity information-sharing program).

149. HARRIS, *supra* note 55, at 130–31.

150. *Id.* at 128–29.

151. *Id.*; *see also id.* at 129 (quoting a former FBI official explaining "[w]e knew what luring words and phrases the e-mails used before they were sent . . . . We told companies what to be on the lookout for. What e-mails not to open. We could tell them 'You're next on the list.'").

152. *Enhanced Cybersecurity Services (ECS)*, DEP'T OF HOMELAND SECURITY, https://www.dhs.gov/enhanced-cybersecurity-services [https://perma.cc/H9E8-Y3US].

153. HARRIS, *supra* note 55, at 168; *see also* Interview by Terry Gross with Shane Harris, Senior Correspondent, The Daily Beast (Nov. 17, 2014), http://www.npr.org/2014/11/17/364718523/an-in-depth-look-at-the-u-s-cyber-war-the-military-alliance-and-its-pitfalls [https://perma.cc/5L4U-KELX] ("Today Lockheed Martin will say that they are tracking as many

The private sector has also begun to act in a coordinated manner to address cybersecurity threats. In October 2014, a coalition of companies, including Cisco, FireEye, iSight Partners, Microsoft, and Novetta, released a report on "Operation SMN."[154] The report explained that the coalition had identified a sophisticated group dubbed "Axiom" that had spied on companies, governments, journalists, and others for over six years, and it alleged that the Axiom group is "part of [the] Chinese Intelligence Apparatus."[155]

What makes the Novetta report different from the Mandiant report and others discussed above is what the companies did about it. The report chronicles the "first industry-led interdiction effort against a sophisticated advanced threat actor group."[156] It explains that, initially, Novetta and Microsoft collaborated to address one of the malware families that Axiom used for its espionage activities, but in order to address a broader swath of Axiom-related malware, they expanded the partnership to "distribute highly sensitive information to 64 trusted industry partners in 22 separate countries for their own use, and to protect their customers."[157] As a result, "over 43,000 separate installations of Axiom-related" malware were removed from computers protected by the partner companies.[158] "Operation SMN" was the first time that "computer security players . . . bond[ed] without using federal or international law enforcement agencies as glue."[159] The senior director of one of the coalition partners declared, "'[t]his is the beginning of what will hopefully be a long line of industry-coordinated efforts to expose these threat groups, and to do so without having to use law enforcement, to help corporations and governments around the world combat' hackers."[160]

Private parties may also be acting independently of the government in undertaking "hacking back," or more euphemistically, "active defense."

---

different hacker groups as the NSA is. They've become almost like an intelligence organization in their own right.").

154. NOVETTA, OPERATION SMN: AXIOM THREAT ACTOR GROUP REPORT (2014), http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf [https://perma.cc/U33U-JSLC]; *see also* Eichensehr, *supra* note 131 (analyzing the report); DJ Summers, *As Cyber Attacks Swell, A Move Toward Improved Industry Collaboration*, FORTUNE (Jan. 7, 2015), http://fortune.com/2015/01/07/cybersecurity-collaboration/ [https://perma.cc/DB3Q-PVCK] (detailing the collaboration that preceded "Operation SMN").

155. Novetta, *supra* note 154, at 4.

156. *Id.* at 5.

157. *Id.*

158. *Id.* at 6.

159. Summers, *supra* note 154.

160. Ellen Nakashima, *Researchers Identify Sophisticated Chinese Cyberespionage Group*, WASH. POST (Oct. 28, 2014), https://www.washingtonpost.com/world/national-security/researchers-identify-sophisticated-chinese-cyberespionage-group/2014/10/27/de30bc9a-5e00-11e4-8b9e-2ccdac31a031_story.html [https://perma.cc/22WN-RRGX] (quoting Stephen Ward, senior director of iSight Partners).

Although the Computer Fraud and Abuse Act prohibits unauthorized access to computers,[161] companies have at times been frustrated with the government's lack of response—or at least lack of direct response—to theft of intellectual property and disruption of corporate networks. Google reportedly hacked a server in 2010 while investigating a compromise by China,[162] and numerous other sources suggest that companies engage in under-the-radar hacking back.[163]

The relationship between the private sector and the government on defense of private networks is complicated. From the government's perspective, the plan is partnership: the Home Depot model where the government gives the private sector information to defend itself, and the government acts as a backstop with criminal prosecutions and sanctions. But at times private sector entities (or at least some of them) have wanted the government to do more, and the government has refused; in other circumstances, the government has wanted to do more, and the private sector has refused. Private networks are now defended by the private sector, with some assistance from the government in the form of information sharing, but as the anecdotes about private intelligence matching the FBI and Operation SMN show, private parties are acting independently of the government and with each other to provide network defense. Network defense now has some elements of partnership, but also elements of role reversal with the private sector deliberately striking out on its own to provide security in a way that looks very governmental.

C. Incentives for Participation in Public-Private Cybersecurity

What drives governmental and private sector participation in the public-private cybersecurity system?

Neither "the government" nor "the private sector" is monolithic. Government agencies have divergent missions and institutional cultures.[164]

---

161. 18 U.S.C. § 1030(a)(2) (2012).

162. *See* HARRIS, *supra* note 55, at 171–72 (relating that Google "traced the intrusion back to what they believe was its source—a server in Taiwan where data was sent after it was siphoned off Google's systems, and that was presumably under the control of hackers in mainland China. 'Google broke in to the server,' says a former senior intelligence official who's familiar with the company's response.").

163. *See, e.g.*, *id.* at 117–18 ("[F]ormer intelligence officials say hack-backs are occurring, even if they're not advertised. 'It is illegal. It is going on,' says a former senior NSA official, now a corporate consultant."); Craig Timberg et al., *Cyberattacks Trigger Talk of 'Hacking Back,'* WASH. POST (Oct. 9, 2014), http://www.washingtonpost.com/business/technology/cyberattacks-trigger-talk-of-hacking-back/2014/10/09/6f0b7a24-4f02-11e4-8c24-487e92bc997b_story.html [https://perma.cc/U94X-YEGJ] (quoting experts noting that hacking back is occurring and alleging "a quiet acceptance on the part of federal agents").

164. *See, e.g.*, AMY B. ZEGART, FLAWED BY DESIGN: THE EVOLUTION OF THE CIA, JCS, AND NSC 20–44 (1999) (discussing divergences between national security and domestic policy agencies

The "private sector" is even more heterogeneous. The companies involved in the case studies in the last subpart include major U.S. technology and software companies, cybersecurity companies, and critical infrastructure institutions, such as banks. These companies are differently situated in many ways. Technology and software companies target worldwide consumer markets and compete partly based on the security of their products. Critical infrastructure companies seek to secure their systems and networks, but unlike cybersecurity companies, they are not primarily in the cybersecurity business.

Although recognizing these distinctions, this subpart identifies some high-level incentives that bridge divisions between different government agencies, on the one hand, and differently situated private sector entities on the other hand.

1. Governmental Incentives.—From the government's perspective, several general reasons support partnering with the private sector or encouraging the private sector to take on government-like responsibilities.

First, in some circumstances, private sector entities can be force multipliers for governmental efforts.[165] Private companies can supply resources and manpower that substitute for resources the government would otherwise have to provide.[166] Botnet takedowns are a good example. When the government engages in a botnet takedown, it has to use its own investigative and legal resources to pursue the case.[167] When Microsoft files a botnet takedown lawsuit, even in conjunction with the United States, Microsoft personnel investigate the botnet,[168] perhaps with government assistance, and then Microsoft's lawyers draft the litigation documents,

---

and among national security agencies); ZETTER, *supra* note 72, at 223 ("[W]ithholding information about vulnerabilities in [U.S.] systems so that they can be exploited in foreign ones creates a schism . . . pit[ting] agencies that hoard and exploit zero days against those, like the Department of Homeland Security, that are supposed to help secure and protect [U.S.] critical infrastructure and government systems."); *supra* note 80.

165. WITTES & BLUM, *supra* note 2, at 71 (arguing that the "distribution of defensive capacity" is "a force multiplier for governments that suddenly have to police a proliferation of ultracapable attackers"); *cf.* DONAHUE & ZECKHAUSER, *supra* note 24, at 32 ("The rationale for involving private players in public work . . . is to amplify government's ability to accomplish its missions.").

166. WITTES & BLUM, *supra* note 2, at 228 (arguing that the government "wants more cybersecurity powerhouses like Mandiant . . . and more online bodyguards hirable by its citizens, and it wants the cadre of highly trained people who are all, or mostly, working in the interests of its own security policies").

167. *See supra* notes 49–53 and accompanying text (discussing the Coreflood botnet takedown).

168. *See supra* note 55 and accompanying text.

supported by affidavits from other Microsoft personnel.[169] Private defense of private networks is another example of the force multiplier effect. General Alexander's request for access to financial institutions' networks notwithstanding, the government does not have the resources to defend all private networks, and therefore relies on private sector entities to defend themselves, perhaps with the assistance of other companies.

Second, in other circumstances, the government may quietly support (or at least not discourage) private action where companies do things that benefit the government while also enabling government deniability. The best examples are the private companies attributing state-sponsored intrusions. The companies' reports bring to light malicious actions by foreign actors, without requiring the government to declassify its own investigations. Whether the attributions occur with minimal coordination with the government or quiet government support, as apparently occurred with Mandiant and with CrowdStrike's attribution of the OPM hack to China, they provide the government with some deniability and may lessen the foreign-relations friction that would occur if the U.S. government made the accusations directly.

The deniability rationale may also undergird the government's approach to securing software, though the rationale is somewhat less direct. Although the government discloses vulnerabilities to companies some of the time,[170] it has generally left software companies responsible for securing their own products. The government does not appear to have assumed a broader software security role by, for example, purchasing large numbers of zero-day vulnerabilities for the purpose of disclosing them.[171] The creation of bug bounty programs—public efforts by private companies to address security flaws—fosters the government's ability to deny that software security is a national security issue for which it should be responsible. Thus, private parties' efforts to better secure software serve the government's interest in preserving a narrow role for itself. This narrative would also support conceiving of the bug bounty programs as another example of a force multiplier: private parties' efforts to secure software are an important

169. For example, Microsoft filed the Citadel botnet takedown documents. *See* Microsoft Corp. v. John Does 1–82, No. 3:13-cv-319 (W.D.N.C. June 5, 2013), http://www.botnetlegalnotice.com/citadel/ [https://perma.cc/5UWS-WBJT] (compiling filings).

170. How much of the time it does and should disclose is a separate issue. *See supra* notes 86–88 and accompanying text.

171. *Cf.* Kim Zetter, *U.S. Gov Insists It Doesn't Stockpile Zero-Day Exploits to Hack Enemies*, WIRED (Nov. 17, 2014), http://www.wired.com/2014/11/michael-daniel-no-zero-day-stockpile/ [https://perma.cc/YBV4-5SBG] (reporting White House Cybersecurity Coordinator Michael Daniel suggesting limited circumstances in which the U.S. government might "purchase some vulnerabilities to disclose" including "if, for example, the government learned that someone was peddling a vulnerability that affected a lot of critical infrastructure networks and the government wanted to take it off the market and get it fixed").

supplement to the government's own efforts to do so (although of course the bounty programs may also plug vulnerabilities that the government would prefer remain open).

Finally, the government has an incentive to cooperate, or at least maintain open lines of communication, with the private sector in order to minimize the risk of companies' actions interfering with government operations and priorities. From the government's perspective, force multiplication by the private sector may be generally positive, but not if the private sector acts without notice to the government and, for example, takes down a botnet that the government is observing for intelligence purposes. Similarly, private attribution of state-sponsored hacks may be helpful in general, but not if a report accusing a foreign country of hacking U.S. businesses were released at a delicate moment, such as, for example, in the middle of negotiations over nuclear weapons. Avoiding operational and diplomatic risk therefore incentivizes the government to keep lines of communication open to the private sector in order to be "in the loop" on what companies may plan to do.

2. Private Incentives.—From the private sector's perspective, the incentives for engaging in government-like actions (with or without partnership with the government) are somewhat different from the government's. Although all companies from small businesses to the top of the Fortune 500 now have cybersecurity concerns, this Article focuses on sophisticated technology and cybersecurity companies because they are the ones engaged in government-like actions. There are differences even among this group—software companies are more consumer-focused, for example—but their sophistication on cybersecurity issues creates some overlap in their motivations, as discussed below.

At the organizational level, business imperatives are the overwhelming impetus for companies' actions. Companies want to defend their networks to avoid theft of intellectual property or other types of corporate espionage, including, for example, the release of potentially embarrassing internal emails.[172] Software companies want to secure their products because a reputation for buggy software can hurt sales and upset existing customers. Botnet takedowns have rested on a legal theory of trademark infringement—harm to a company's intellectual property—as well as harm to customers from malware infections due to flaws in the company's software.[173]

---

172. *See, e.g.*, Amy Kaufman, *The Embarrassing Emails that Preceded Amy Pascal's Resignation*, L.A. TIMES (Feb. 5, 2015), http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-amy-pascal-email-rogen-hirai-20150205-story.html [https://perma.cc/Z2XY-SWF7] (reporting on emails from Sony Pictures Entertainment's co-chair that were leaked as part of the 2014 Sony hack).

173. *See supra* notes 45–46 and accompanying text.

Relatedly, the public-relations benefits of some of the actions are substantial. For example, attributing cyber intrusions to state-sponsored attackers is excellent advertising.[174] Accusing foreign governments of hacking generates media attention, and companies benefit from subsequent references to their reports by government officials, seemingly corroborating the companies' accusations and bolstering their credibility.[175] Botnet takedowns have also received positive press coverage, giving companies an opportunity to tout their dedication to consumer protection.[176] Bug bounty programs have a public-relations component as well. They can help a company to preserve or improve relationships with computer-security researchers who want to use their skills to secure software, rather than profiting on the black or gray markets (i.e., "white-hat" hackers). Companies that do *not* have bounty programs have faced criticism for failing to reward researchers who help the company.[177]

Setting aside the organizational-level incentives, at the individual level, at least some employees within the companies are likely motivated by personal incentives, including community attachments.[178] For example, personal ties to security researchers could make employees more willing to reward the researchers' work. Identification with the community of Internet

174. *See, e.g.*, Jim Finkle, *Mandiant Goes Viral After China Hacking Report*, REUTERS (Feb. 22, 2013), http://www.reuters.com/article/net-us-hackers-virus-china-mandiant-idUSBRE91M02P20130223 [https://perma.cc/EQ57-862F] (noting that "Mandiant was largely unknown outside the computer security industry" until the APT1 report); *FireEye Acquires Mandiant in $1bn Deal*, BBC (Jan. 3, 2014), http://www.bbc.com/news/business-25584644 [https://perma.cc/EG3C-7X9D] (noting that Mandiant "rose to prominence" due to the APT1 report); *see also supra* note 135.

175. Reports accusing foreign governments of wrongdoing are not without risk. For example, Norse, a "cyber intelligence firm," claimed that it had evidence that a disgruntled employee, not North Korea, was responsible for the Sony hack, but the FBI publicly rejected Norse's claim. Tal Kopan, *FBI Rejects Alternate Sony Hack Theory*, POLITICO (Dec. 30, 2014), http://www.politico.com/story/2014/12/fbi-rejects-alternate-sony-hack-theory-113893.html [https://perma.cc/H3C3-MD7Y].

176. For positive press coverage of takedown operations, see, for example, *FBI and Microsoft Take Down $500m-Theft Botnet Citadel*, BBC (June 6, 2013), http://www.bbc.com/news/technology-22795074 [https://perma.cc/B8MJ-RGH6]; Nick Wingfield & Nicole Perlroth, *Microsoft Raids Tackle Internet Crime*, N.Y. TIMES (Mar. 26, 2012), http://www.nytimes.com/2012/03/26/technology/microsoft-raids-tackle-online-crime.html [https://perma.cc/GDU6-ZW46].

177. *See, e.g.*, Dennis Fisher, *No More Free Bugs for Software Vendors*, THREATPOST (Mar. 23, 2009), https://threatpost.com/no-more-free-bugs-software-vendors-032309/72484 [https://perma.cc/DWX6-WERB] (highlighting "no more free bugs" movement among security researchers and arguing that companies "shouldn't expect the bug finder to just hand over the details gratis" rather than selling the vulnerability).

178. *See* Martha Finnemore & Duncan B. Hollis, *Constructing Norms for Global Cybersecurity*, 110 AM. J. INT'L L. 425, 442–43 (2016) (discussing the "culture of Silicon Valley—with its emphasis on security and privacy"); *see also id.* at 461 (discussing "cultural norms" that "dispose technologists toward particular views of the role that digital technology can or should play in society").

users could make employees want to protect other users by eliminating malware infections and botnets that exploit individuals. Personal and professional ties to the U.S. government may also have a significant incentivizing effect. Many cybersecurity companies are staffed by former government officials.[179] Their ties to the government may make cooperation easier; for example, cooperation and coordination may involve meeting with former colleagues. Similarly, former government officials may be motivated by a continuing patriotic impulse to "do their part" for the United States in investigating particular intrusions, timing the release of reports, or sharing information with the government.[180]

* * *

The interests of the government and private sector often align, fostering coordination, cooperation, and even de facto outsourcing to the private sector. Both the government and companies benefit from their alignment, though of course their interests are not always in sync.[181] The next Part turns from governmental and private interests to public values.

II. Privatization & Public Law Values

The increasing transfer of government functions to private actors in recent decades has sparked academic and popular debate about privatization.[182] Although "privatization" can describe a variety of situations,[183] many legal scholars focus on privatization through "contracting

179. *See, e.g.*, Ellen Nakashima, *The Latest Hot Job in the Washington Revolving Door? Cybersecurity*, WASH. POST (Mar. 17, 2015), http://www.washingtonpost.com/blogs/in-the-loop/wp/2015/03/17/the-latest-hot-job-in-the-washington-revolving-door-cybersecurity/ [https://perma.cc/7F8R-42BF]; Tim Shorrock, *How Private Contractors Have Created a Shadow NSA*, NATION (May 27, 2015), http://www.thenation.com/article/how-private-contractors-have-created-shadow-nsa/ [https://perma.cc/6GZH-SYCG].

180. *Cf.* Michaels, *supra* note 17, at 927–28 (describing how intelligence agencies "make appeals to CEOs' personal vanities, friendship, or sense of patriotism" to convince them to assist the government informally).

181. *See, e.g.*, *supra* notes 142–44 and accompanying text.

182. *See, e.g.*, Martha Minow, *Public and Private Partnerships: Accounting for the New Religion*, 116 HARV. L. REV. 1229, 1229 (2003) (exploring "[w]hat happens to the scope and content of public values when public commitments proceed through private agents").

183. As a general matter, "privatization" "denotes a broad spectrum of adjustments to the interaction between government and various private actors," Jack M. Beermann, *Privatization and Political Accountability*, 28 FORDHAM URB. L.J. 1507, 1508 (2001), particularly "the range of efforts by governments to move public functions into private hands and to use market-style competition." Minow, *supra* note 182, at 1230; *see also* Freeman, *supra* note 24, at 1287 (arguing that "privatization" "describes nothing in particular so much as it suggests a host of arrangements," including "(1) the complete or partial sell-off . . . of major public enterprises; (2) the deregulation of a particular industry; (3) the commercialization of a government department; (4) the removal of subsidies to producers; and (5) the assumption by private operators of what were formerly exclusively public services," such as through "contracting out").

out" of government services to private entities.[184] They address situations like private prisons and military contractors where private parties sign a contract with the federal government to deliver a service that the government had previously performed.[185]

In these privatization scenarios, scholars have focused on what tasks may be outsourced and whether transferring governmental functions to private actors undermines public law values, such as accountability, transparency, and fairness.[186] These concerns stem from structural differences between the government and private actors. Governmental actors operate in a system of structural checks that, although imperfect, constrains their actions. Government officials may be held accountable through congressional oversight and elections either of themselves or of higher level

184. *See, e.g.*, Nina A. Mendelson, *Six Simple Steps to Increase Contractor Accountability*, *in* GOVERNMENT BY CONTRACT: OUTSOURCING AND AMERICAN DEMOCRACY 241, 241 (Jody Freeman & Martha Minow eds., 2009) (focusing on "services contracts"); Freeman, *supra* note 24, at 1286–87 (focusing exclusively on "contracting out" because it is the "most common" form of privatization in the United States); Jon D. Michaels, *Privatization's Pretensions*, 77 U. CHI. L. REV. 717, 717 n.1 (2010) (recognizing that privatization can describe other practices, but equating privatization and contracting out); Martha Minow, *Outsourcing Power: How Privatizing Military Efforts Challenges Accountability, Professionalism, and Democracy*, 46 B.C. L. REV. 989, 997–98 (2005) (explaining that privatization often means contracting out—"reliance on nongovernmental actors who are paid under publicly-funded contracts"). *But see* Joh, *supra* note 25, at 586–87 ("[O]nly some private policing is contracted out by cost-conscious public agencies. . . . [P]rivate police often operate wholly outside of direct public management." (footnote omitted)). Scholarly interest in the role of private parties is not limited to legal scholars. *See, e.g.*, DONAHUE & ZECKHAUSER, *supra* note 24, at 6–8 (highlighting relevant literature from political science, economics, business, and public management). Legal scholars, however, address privatization and related issues "in a language all their own." *Id.* at 6. This Article, too, speaks primarily that legal language.

185. *See, e.g.*, Dickinson, *supra* note 24, at 390 (discussing privatization in foreign relations, including military contractors); Sharon Dolovich, *State Punishment and Private Prisons*, 55 DUKE L.J. 437 (2005) (assessing the legitimacy of private prisons).

186. *See, e.g.*, Custos & Reitz, *supra* note 36, at 556 (identifying as one of the "most important deficiencies in current law" the failure "to extend the public values of administrative law" to public-private partnerships); Laura A. Dickinson, *Outsourcing Covert Activities*, 5 J. NAT'L SECURITY L. & POL'Y 521, 522 (2012) (arguing that "[t]he ever-expanding use of contractors threatens core public values because the mechanisms of accountability and oversight that the United States has generally used to curb abuses by government employees do not translate well to contractors"); Dolovich, *supra* note 185, at 442–43 (discussing the idea that "incarceration is an inherently public function and thus that recourse to private prisons is inappropriate regardless of the relative efficiency of this penal form"); Michaels, *supra* note 184, at 729 (identifying as "dominant worries about government contracting . . . whether the responsibilities being outsourced are inherently governmental (and thus unsuitable for delegation to private actors), whether contractors are more efficient than their government counterparts, and whether contractors are accountable agents" (footnote omitted)); Minow, *supra* note 182, at 1229 (exploring "[w]hat happens to the scope and content of public values when public commitments proceed through private agents").

officials who are responsible for the actions of the bureaucracy.[187] They are constrained by legal obligations, such as requirements of due process and equal protection.[188] Government actions are also subject to scrutiny through mechanisms such as freedom-of-information requests and investigations by Congress or agency inspectors general.[189]

Private actors, on the other hand, are not subject to these constraints, even when undertaking government-like functions. The absence of such restrictions sparks fears that private parties are more likely to abuse the power they exercise and that government officials may contract out particular functions precisely because private contractors have more freedom to act.[190] Even apart from concerns about abuse of power, some commentators also question the legitimacy of private parties performing government-like actions, particularly when they involve discretionary policy choices.[191]

Pushing back against the concerns that private contractors necessarily undermine public law values, Jody Freeman has proposed that private contracting might actually advance public law norms through a process she terms "publicization."[192] Through publicization, private contractors would "increasingly commit themselves to traditionally public goals as the price of access to lucrative opportunities to deliver goods and services that might otherwise be provided directly by the state."[193] As a result, publicization would "*enhance* public law norms by extending them to realms where they typically do not play a significant role."[194] Other scholars have in effect adapted Freeman's publicization concept to particular contexts, such as military contractors and private-intelligence partnerships, and similarly

187. *See, e.g.*, Minow, *supra* note 182, at 1263 (describing accountability mechanisms that constrain democratic governments including transparency, public debate, and "the electoral sanction").

188. U.S. CONST. amends. V, XIV.

189. *See, e.g.*, Mendelson, *supra* note 184, at 244–53 (comparing legal constraints on government agencies versus on contractors); Shirin Sinnar, *Protecting Rights from Within? Inspectors General and National Security Oversight*, 65 STAN. L. REV. 1027, 1031 (2013) (highlighting the role of agency inspectors general in monitoring even national security agencies).

190. *See, e.g.*, Custos & Reitz, *supra* note 36, at 577 (arguing that "[c]ontracting out is . . . all too susceptible to being abused as a way to evade the complex of public values imposed by public law"); Freeman, *supra* note 24, at 1304 ("Public law scholars worry that privatization may enable government to avoid its traditional legal obligations, leading to an erosion of public law norms and a systematic failure of public accountability.").

191. Freeman, *supra* note 24, at 1343 (describing the public law perspective as "concerned about the political legitimacy of conferring policymaking discretion on nongovernmental actors").

192. *Id.* at 1314–15.

193. *Id.* at 1285.

194. *Id.* at 1314.

argued that private parties can be co-opted to support and enhance, rather than undermine, public law values.[195]

The public-private cybersecurity system shares some features with traditional privatization scenarios. In particular, it involves private actors performing government-like roles, and it therefore triggers similar questions about whether private actors are serving or can be made to serve public law values. But the public-private role reversals and informality of the public-private cybersecurity system pose both procedural and substantive challenges to conventional accounts of privatization and to their prescriptions for protecting public law values. The structure of the public-private relationships in cybersecurity renders the usual concerns at once more serious and more difficult to remedy.

Subpart II(A) identifies several procedural challenges that public-private cybersecurity raises for the extant legal literature on privatization. Subpart II(B) highlights the substantive public values that cybersecurity implicates, drawing from and broadening the list of values addressed in most studies of privatization.

A. The Procedural Challenges of Public-Private Cybersecurity

The public-private cybersecurity system challenges existing scholarly accounts of privatization on at least three procedural grounds, that is, grounds related to how government-private sector relations function.

First, in traditional privatization, the government decides whether private actors should perform a particular function; in public-private cybersecurity, however, private actors decide for themselves which functions they should perform.

In a typical privatization context, the government performs a certain function, decides that the function can or should be outsourced, and contracts with a private actor, who then takes up performance. Office of Management and Budget Circular No. A-76, discussed above,[196] illustrates the normal situation in which the government holds powers *ab initio* and decides

---

195. *See, e.g.*, Dickinson, *supra* note 186, at 536 (observing that "privatization may actually create some interesting and surprising spaces where public law values may be protected, and perhaps even expanded"); Dickinson, *supra* note 24, at 385 n.18 (arguing that "[i]nstead of seeing privatization solely as a threat to public values[,] . . . we should focus on the negotiated contractual relationships between the public and the private" as a way to "harness[] private capacity to serve public goals") (quoting Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. REV. 543, 549 (2000)); Mendelson, *supra* note 184, at 243 (arguing that well-designed contracts and "[c]lose agency supervision of a contractor could, in theory, provide a functional substitute for other forms of public and legal accountability"); *cf.* Michaels, *supra* note 17, at 947–48 (arguing that "privatization in the intelligence-gathering context can be accountability enhancing" precisely because private companies do not share the government's counterterrorism agenda and may therefore be "less likely to disregard the law in the name of national security").

196. *See supra* notes 30–34 and accompanying text.

whether and how much to delegate to private actors. In other words, the government acts as a gatekeeper in making the initial decision of what activities are "inherently governmental"—and therefore inappropriate for private actors.

The same is true even in informal partnerships, such as those described by Jon Michaels in the counterterrorism context. Michaels's work focuses on private "actors who have been invited or solicited in their capacities as corporate executives or employees to provide counterterrorism assistance to the government"—and excludes "those operating pursuant to government contracts to assist in homeland security programs, or those compelled to support investigations through legal instruments such as court orders, subpoenas, or regulatory directives."[197] Although Michaels addresses noncontractual collaborations,[198] the relationships he describes still have the government in a gatekeeping role: the government solicits assistance from the private sector, and that assistance allows the *government* to engage in quintessentially governmental activity.

Public-private cybersecurity does not abide by this government-directed structure. In the cybersecurity context, the metaquestion of who decides who will perform various functions often rests with private actors.[199] In many cybersecurity contexts, there was no "time zero" at which the government did all of the things that the private sector now undertakes. Empowered private sector actors have determined for themselves what actions they can and should perform, and in doing so, they implicitly assert that certain functions are not inherently governmental.

The absence of government gatekeeping in public-private cybersecurity resembles some instances of private policing. As Elizabeth Joh has noted, "[m]uch private policing arises from the private sector to meet private demands," rather than coming through direct delegations and contracting relationships from public police agencies.[200] Examples include contract guards and corporate police who protect the hiring company's property and

197. Jon D. Michaels, *Deputizing Homeland Security*, 88 TEXAS L. REV. 1435, 1442 (2010).

198. Michaels, *supra* note 17, at 901 (noting that the collaborations are "orchestrated around handshakes rather than legal formalities").

199. This feature distinguishes public-private cybersecurity not just from formal contracting, but also from less formal instances of "collaborative governance," which still assume ultimate government control. *See* DONAHUE & ZECKHAUSER, *supra* note 24, at 31 ("Collaborative governance can be thought of as a form of agency relationship between government as principal and private players as agents. The same is true of simple contracting, but in those sorts of arrangements the governmental principal aims to impose firm control. In collaborative governance, . . . the governmental principal willingly grants its agent a certain amount of discretion.").

200. Joh, *supra* note 25, at 587; *see also id.* at 611–15 (proposing a four-part typology for private policing, only one type of which is "publicly contracted policing," wherein "a private police agency replaces a *specific* service formerly performed by the government").

guard the safety of those on it.[201] These instances of private policing are generated and controlled by private actors, like the private sector's cybersecurity endeavors.

Yet private actions in cybersecurity differ from private policing. Private companies' cybersecurity-related actions are typically geographically and jurisdictionally broader than the scope of corporate policing. As the examples in Part I show, many of the private sector's actions in cybersecurity are outward-facing, stretching well beyond a company's own property, carrying national and cross-border effect, and in some cases running the risk of sparking international incidents. Moreover, the nature of the correspondence between the private parties' role and the government's also differs. In private policing, the private actors are duplicating and making more particular the protective functions the government performs—corporate police supplement local, state, and federal law enforcement. In the cybersecurity context, on the other hand, private actors have innovated some of the functions they perform—the government did not perform them first, or perhaps at all.

The second procedural challenge the public-private cybersecurity system poses for existing theories of privatization similarly stems from the government's absence from its traditional gatekeeping role. The existing legal literature—responding no doubt to the scenarios that motivated it—focuses overwhelmingly on formal outsourcing via contract.[202] And it relies on the existence of formal contracts to remedy concerns about whether private actors comply with public law values, like accountability and fairness, that apply to governmental actors.[203] For example, in considering military and intelligence contractors, Laura Dickinson has proposed that "contracts

---

201. *Id.* at 610–11, 615 (describing "protective policing" and "corporate policing"). Joh discusses an additional category of "intelligence policing," which includes, for example, the work of private investigators. *See id.* at 611–13. The work of cybersecurity-forensics firms in investigating intrusions at the behest of client companies may be a cybersecurity analogue.

202. *See supra* note 184 and accompanying text. A major exception is Jon Michaels's work on informal partnerships in the intelligence context. *See supra* notes 197–98 and accompanying text.

203. *See, e.g.*, Custos & Reitz, *supra* note 36, at 579 (arguing that while "contract law is a large part of the problem because it does not adequately protect public values, it could also be the solution" if contracts are used to impose public law requirements on contractors); Dickinson, *supra* note 24, at 388, 402 (focusing on government contracting and proposing nine ways that contracts can be used as a vehicle for remedying concerns with privatization); Freeman, *supra* note 24, at 1334 ("While some species of private decisionmaking may not easily submit to judicial review, as long as there are contracts, regulations, and grant conditions to enforce, courts will be a possible venue for those seeking to protect public law norms." (footnote omitted)); Mendelson, *supra* note 184, at 254 (suggesting contracts can improve transparency by requiring greater disclosures regarding contractors' actions); Sklansky, *supra* note 25, at 93 ("[A]s long as government is paying for law enforcement it retains control of fundamental questions of allocation, and the outsourcing contract may provide a particularly promising vehicle for applying 'public law norms' to private policing."). *But see* Dolovich, *supra* note 185, at 477–80 (expressing skepticism about the efficacy of contractual restrictions as a check on private prison operators).

should explicitly require that contractors obey norms and rules that implement public law values."[204] In particular, she argues, contracts could improve accountability by "explicitly extend[ing] the norms of public international law to contractors . . . , provid[ing] more specific terms (such as training requirements and performance benchmarks), assur[ing] better monitoring and oversight, requir[ing] contractors to submit to outside accreditation by third-party organizations, and offer[ing] better enforcement mechanisms, such as third-party beneficiary suits."[205]

The public-private collaborations in the cybersecurity context are not susceptible to similar remedies. As described in Part I, the public-private collaborations in cybersecurity are informal, de facto partnerships, operating outside a contracting framework. The informality in the cybersecurity context renders the privatization literature's specific prescriptions about incorporating public law values into private contracts inapplicable.

Moreover, not only are the cybersecurity relationships *currently* informal but in many instances neither the government nor the private actors would want to formalize their relationships into contracts going forward. Both the government and the private sector benefit from the lack of formal relationship. The private actors do not necessarily want to operate as agents of the government, with the supervision, potential public-relations consequences, and possible legal liabilities that would trigger. The government, on the other hand, would not want to pay for actions that the private sector currently undertakes for free and may prefer to maintain deniability for some private actions.

The final procedural challenge that public-private cybersecurity poses for traditional privatization literature also relates to the absence of formal contractual relations, but focuses on the back end of the government–private sector relationship: the absence of a contractual relationship limits the government's ability to pull power away from the private sector and back to the government. In traditional contracting out, the government delegates power to a private actor for the duration of the contract, and at the contract's expiration, the government has a decision point where it determines whether to renew the contract or not. The moment of contract renewal or nonrenewal presents an opportunity for the government to reel back in power that it has delegated. The absence of contractual relationships in public-private cybersecurity removes this decisional moment and the opportunity for the government to reconsider and readjust the balance of public-private power.

---

204. Dickinson, *supra* note 186, at 529.

205. *Id.* at 525–26; *see also* Dickinson, *supra* note 24, at 403 (providing similar suggestions); Sklansky, *supra* note 25, at 91 (explaining that for private policing, "[i]n the not uncommon situation where government itself is the purchaser, 'public norms' can be imposed by contract").

In sum, in public-private cybersecurity, unlike traditional contracting out or even prior instances of informal public-private partnerships, the government does not determine what functions private actors may undertake. Because the government does not play an initial gatekeeping role, it also lacks the ability to control private actors via contracts—the mechanism that privatization scholars have endorsed as a means of "publicizing" private actors performing governmental functions. And it does not have a routinized, periodic process to reconsider delegations of power to private actors. The absence of the government as an initial check on what actions the private sector may perform in the cybersecurity context makes evaluation of whether private actors are serving public law values more important, but it also renders remedial steps more complex because such measures cannot simply be baked into a governing contract. As a result, private sector actors in cybersecurity now decide what functions they should perform, how they should do them, whether and how much to consider public law values, and how to adjudicate tradeoffs between competing values.

B. Expanding Public Law Values for Cybersecurity

The existing privatization literature has identified a number of public law values that scholars believe may be put at risk when the government transfers responsibilities to the private sector. Privatization scholars focus primarily on accountability and secondarily on transparency and fairness or due process.[206] The public-private cybersecurity system implicates these values, but it also brings to the fore additional concepts that are arguably public law values or at least public goods. To conceptualize the full range of values at play in public-private cybersecurity therefore requires broadening the scope of the existing privatization literature.

This subpart explores five key values at issue in cybersecurity: accountability, transparency, due process or fairness, security, and privacy.[207] The values overlap in some instances. For example, transparency can foster accountability, which in turn may ensure fairness and protect privacy. In

206. *See, e.g.*, Laura A. Dickinson, *Regulating the Privatized Security Industry: The Promise of Public/Private Governance*, 63 EMORY L.J. 417, 419 (2013) (identifying "core public values" as "substantively, the values of human dignity embedded in human rights and humanitarian law, as well as the procedural values of global administrative law: public participation, transparency, and accountability"); Freeman, *supra* note 24, at 1285 (identifying "democratic norms of accountability, due process, equality, and rationality").

207. Literature on privatization often discusses efficiency as an additional value, and typically as an argument in favor of privatization. Likely due to efficiency's preexisting association with the private sector, it does not appear in discussions of *public* values with respect to privatization. *Cf.* INS v. Chadha, 462 U.S. 919, 958–59 (1983) ("[I]t is crystal clear . . . that the Framers ranked other values higher than efficiency."); Jon D. Michaels, *An Enduring, Evolving Separation of Powers*, 115 COLUM. L. REV. 515, 572 (2015) ("For better or worse, efficiency is not considered a preeminent constitutional value . . . .").

other instances, the values may conflict. For example, full, public transparency in accusations about the source of particular cyberattacks could endanger security by compromising intelligence sources and methods. Differing conceptions of a single value may even be in tension, such as when companies seek to patch software to protect the security of individual users, while governments seek to use the same vulnerabilities for criminal investigations, espionage, or offensive operations in the service of national security.[208] Nonetheless, addressing the values separately helps to clarify the core contribution of each one and provides analytical clarity to evaluate whether and how the public-private cybersecurity system puts the values at risk.

Moreover, the exploration of each value is necessarily brief. In keeping with the Article's aim to identify the range of values implicated, rather than to provide an exhaustive treatment of each one, this subpart focuses on how the role of empowered private parties complicates the nature and operation of the public law values.

1. Accountability.—Accountability in the privatization literature is a broad concept.[209] Martha Minow defines "accountability" as "being answerable to authority that can mandate desirable conduct and sanction conduct that breaches identified obligations."[210] In a democratic system, "the ultimate authority should be the general population."[211] Accountability has both ongoing and retrospective components. On an ongoing basis, accountability "entails some form of ongoing scrutiny over those carrying out an activity to ensure that those actors fulfill the purposes as specified."[212] Retrospective accountability, or "accountability as redress," by contrast, means that an authority "imposes a penalty if a person or organization has

208. The Apple–FBI controversy provides an example of such a security–security tradeoff. *See supra* notes 95–99; *cf.* David E. Pozen, *Privacy-Privacy Tradeoffs*, 83 U. CHI. L. REV. 221, 222 (2016) (discussing "privacy-privacy tradeoffs" where "privacy . . . clashes with itself").

209. Some definitions of accountability use it as an umbrella concept to include arguably separate values, such as transparency and public participation. *See, e.g.*, Beermann, *supra* note 183, at 1509 ("Political accountability should be understood to include the democratic character of decision-making, the clarity of responsibility for an action or policy within the political system, and the ability of the body politic to obtain accurate information about a governmental policy or action."); Minow, *supra* note 182, at 1259 (identifying "public values of fairness, equality, and neutrality," preserved through maintaining accountability, and identifying the "urgent question posed by a shifting mix of public and private providers of" formerly governmental services as "how to ensure genuine and ongoing accountability to the public").

210. Minow, *supra* note 182, at 1260; *see also* Beermann, *supra* note 183, at 1507 ("Political accountability is to be understood as the amenability of a government policy or activity to monitoring through the political process.").

211. Minow, *supra* note 182, at 1260.

212. Dickinson, *supra* note 206, at 435–36 (discussing "accountability as managerial oversight").

failed to comply with a particular rule or standard."[213] In other words, retrospective accountability is the idea that when something goes wrong, "there is somewhere to go after the fact to punish wrongdoers."[214] Governments are subject (at least in theory) to both types of accountability. For example, voters review government officials' performance on an ongoing basis in elections, and aggrieved individuals can file lawsuits to challenge government actions after the fact.

Privatizing government functions, however, can undermine both types of accountability. Private actors are not subject to requirements like the Administrative Procedure Act,[215] due process, and equal protection that could form the grounds for an after-the-fact lawsuit challenging governmental action. Privatization can also impair ongoing accountability by obfuscating who is responsible for certain actions, creating confusion about whether an action is attributable to the government at all and, if so, which government entity has authority to remedy the perceived harm.[216] This is a particular concern when collaborations are informal. Not only are informal collaborations difficult for the public to discover and understand, but they also impair ongoing oversight by Congress, potentially creating an "accountability gap."[217] In other words, "Congress cannot effectively monitor—let alone interfere with—that which is not disclosed to it."[218]

To be sure, private actors do face some accountability mechanisms. They are subject to market competition, scrutiny from investors, legal and regulatory curbs on their behavior, and (at least for publicly traded companies) disclosure requirements.[219] They may also be subject to tort claims from which the government has immunity.[220] Proponents of privatization argue that these accountability mechanisms are *more* effective and more important than the accountability mechanisms that apply to public

213. *Id.* at 435.

214. *Id.*

215. 5 U.S.C. § 553 (2012).

216. *See, e.g.*, Beermann, *supra* note 183, at 1519 ("[I]f a private entity were entrusted with carrying out a government activity, it might be difficult for the public to know whom in the political system to blame when things go wrong.").

217. Michaels, *supra* note 17, at 932 (arguing that informal intelligence-gathering partnerships produce an "accountability gap" because they are "masked from Congress and the courts").

218. *Id.* at 924; *see also id.* (explaining that because of the informality of intelligence partnerships, "Congress is not well-positioned to investigate intelligence operations, interrogate corporate executives about their involvement in the partnerships, demand some showing of success, withhold funding, or insist that the parties take specific measures to safeguard against, among other things, unnecessary or excessive privacy intrusions").

219. *See* Minow, *supra* note 182, at 1263 (detailing these and other accountability mechanisms operative on private actors).

220. *See, e.g.*, Freeman, *supra* note 24, at 1321 ("[P]rivate actors are generally more vulnerable to tort liability than public entities.").

actors.[221] The presence of private accountability mechanisms, however, does not change the fact that private actors largely escape public accountability mechanisms.

2. Transparency.—Transparency is another core public law value.[222] Transparency "refers to the availability of information about government policies, structures, and actions."[223] Transparency about government operations ensures that citizens can be informed about actions undertaken by their democratic representatives, and it therefore permits "a feedback loop between government actors and those affected by government policy."[224] Such feedback is particularly important for bureaucratic officials who do not stand for election. In this way, transparency fosters accountability by providing the information necessary to supervise officials.[225] Correspondingly, a lack of transparency impairs public deliberation and oversight.[226]

Transparency may have benefits beyond accountability. It is a long-standing tenet of legal theory in the United States that, in Justice Brandeis's famous phrase, "sunlight is . . . the best of disinfectants."[227] Transparency may substantively alter and improve the quality of decisions taken in the shadow of disclosure requirements[228] as well as strengthen public confidence

221. *See* Trebilcock & Iacobucci, *supra* note 26, at 1447–49 (describing and arguing in favor of the efficacy of private-accountability mechanisms).

222. *See, e.g.*, Dickinson, *supra* note 206, at 434 (listing transparency as a "core value in the global administrative space"); Erik Luna, *Transparent Policing*, 85 IOWA L. REV. 1107, 1164 (2000) (declaring transparency "a well-developed norm of democratic government"); Anne Joseph O'Connell, *The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World*, 94 CALIF. L. REV. 1655, 1716 (2006) (listing transparency as one of the core values "fundamental to our society").

223. O'Connell, *supra* note 222, at 1717.

224. Dickinson, *supra* note 206, at 434.

225. O'Connell, *supra* note 222, at 1717 (arguing that availability of information about government actions "helps citizens (and others) assess and attempt to change their government's performance").

226. *See, e.g.*, Minow, *supra* note 184, at 1000 (noting that lack of transparency about the role of military contractors inhibits assessment of "how well the contractors are performing, how well they are achieving goals of military purposes, and how well they are achieving goals of a constitutional democracy").

227. LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY AND HOW THE BANKERS USE IT 92 (1914).

228. *See, e.g.*, Mark Fenster, *The Opacity of Transparency*, 91 IOWA L. REV. 885, 900 (2006) (arguing that transparency "enables the free flow of information among public agencies and private individuals, allowing input, review, and criticism of government action, and thereby increases the quality of governance"); Luna, *supra* note 222, at 1164 (arguing in favor of transparency because "[s]uperior judgments can only be reached through the free circulation of knowledge between the government and the governed").

in decisions that result from the process.[229] The knowledge that a decision will be disclosed may also insulate it from corrupt influences and deter rights violations.

The transparency mechanisms that operate on the federal government do not apply to private parties performing governmental functions, whether under formal contracts or in the informal situations at issue in cybersecurity. For example, much government-agency policymaking is subject to notice-and-comment rulemaking, requiring the disclosure of proposed policies and an opportunity for public feedback.[230] Agencies are also required to make materials available pursuant to the Freedom of Information Act (FOIA).[231] These statutes, however, do not reach government contractors,[232] much less informal partners or private parties acting independently of the government but in a government-like fashion.

In addition to the specific problems of transparency regarding the actions of private parties, transparency poses particular challenges in areas like foreign policy, national security, and military operations. This is true even when the government itself acts. The Administrative Procedure Act specifically exempts "military" and "foreign affairs function[s]" from the requirements of notice-and-comment rulemaking,[233] and FOIA includes an exemption for classified information related to "national defense or foreign policy."[234] Secrecy may be crucial to effective action in these areas, but it is also in some tension with the ideal of an informed and engaged public.

Nonetheless, as discussed in Part III, in at least some circumstances, a balance can be struck to capture some of the benefits of transparency without sacrificing security. For example, disclosure may include general outlines of a policy, but not operational details.[235] Or public disclosure may be delayed to preserve operational effectiveness, but still permit after-the-fact review.[236]

---

229. *See, e.g.*, Sierra Club v. Costle, 657 F.2d 298, 400 (D.C. Cir. 1981) (noting that the "very legitimacy" of agency policymaking "depends in no small part upon the openness, accessibility, and amenability of these [agency] officials to the needs and ideas of the public"); Luna, *supra* note 222, at 1165 (noting that the Administrative Procedure Act "mandate[s] specific rulemaking procedures and rules of disclosure as a means of instilling public confidence through rational process and accessibility").

230. Administrative Procedure Act § 4, 5 U.S.C. § 553 (2012).

231. Freedom of Information Act, 5 U.S.C.A. § 552 (West 2016).

232. *See, e.g.*, Mendelson, *supra* note 184, at 249–50 (explaining the limits of the Administrative Procedure Act and the Freedom of Information Act and why the statutes do not cover government contractors).

233. 5 U.S.C. § 553(a)(1).

234. 5 U.S.C.A. § 552(b)(1).

235. *See supra* notes 86–88 and accompanying text; *infra* notes 280–85 and accompanying text.

236. *See infra* notes 265–67 and accompanying text.

3. Due Process & Fairness.—A third public law value is the concept of due process or fairness. At the most micro-level, due process addresses whether individuals are treated fairly and in accordance with applicable procedural requirements.[237] For example, when an individual is deprived of liberty or property, due process requires certain procedures, such as notice and an opportunity to challenge the deprivation.[238]

Broadening the lens slightly, the idea of fairness may also apply to citizens at an aggregate level. Governments routinely make decisions about the allocation of resources to different areas and about the prioritization of competing imperatives in the face of scarce resources. Such decisions can spur more macro-level fairness questions, even if they do not violate individual-level due process rights.[239] For example, in a noncybersecurity context, a government may decide to allocate additional police patrols to a particular neighborhood, with the effect that the neighborhood with the additional patrols benefits from a lower crime rate than surrounding areas. Transposed to the cybersecurity context, macro-level fairness questions can arise when the government decides to provide more cybersecurity threat information to one industry than to another, although both are suffering major losses from cyber intrusions. Or fairness questions may arise from the decision to focus on taking down one botnet to the exclusion of another.

While governments are routinely trusted with discretionary decisions about public resource allocation, private parties are not. Private parties typically make decisions about allocating *their own* resources. When private parties are providing public goods or public services, however, their actions should arguably account for the same values, like fairness or due process, that governments are expected to deploy in allocating public resources. How exactly to implement such value determinations in the cybersecurity context is complex. The accountability mechanisms that operate on governments, from elections to legal limits on governmental action, do not restrain private actors in the same way, even when the private actors are acting like governments in deciding how to allocate security.

4. Security.—In addition to the public law values already discussed, citizens expect their government to provide security. National security is a

---

237. Beermann, *supra* note 183, at 1528 (conceiving of due process as "accountability writ small" because "it is concerned with correctness and fairness in individual decisions, not with accountability to the body politic generally"); Sklansky, *supra* note 23, at 1280 (describing due process as "fairness writ small").

238. Hamdi v. Rumsfeld, 542 U.S. 507, 528–29 (2004) (plurality opinion) (describing the *Mathews v. Eldridge*, 424 U.S. 319 (1976), test for due process protections).

239. *See* Sklansky, *supra* note 23, at 1280–83 (discussing the "equitable allocation of criminal justice resources" as a question of fairness, despite the Supreme Court's refusal to "recognize a right to minimally adequate protection under the Due Process Clauses").

public good,[240] and is often cited as the quintessential public good.[241] Although security is a "public good" and not precisely a "public value," like accountability and transparency, it merits consideration here because it falls in the broader category of things government is expected to provide to citizens. And the provision of security may clash with the public law values, like accountability and transparency, that the government is also expected to satisfy.

The government often engages in public-private partnerships or contracts with the private sector in order to fulfill its duty to provide national security. It outsources or engages partners in security functions when, at least in theory, doing so improves security or provides security more efficiently than government acting alone. Partnering with the private sector should ideally improve security, such as when private entities act as force multipliers for the government.[242]

However, privatization and public-private partnerships in the national security arena may also challenge the conventional understanding that the state is responsible for providing the public good of national security. The basic logic of the Westphalian-state system rests on *states*' responsibility for securing their borders and their citizens within those borders.[243] Having private actors undertake government-like activities in partnership with, or

240. Public goods are ones that are nonrivalrous and nonexcludable. *See* MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS 14 (20th prtg. 2002) ("The basic and most elementary goods or services provided by government, like defense and police protection, and the system of law and order generally, are such that they go to everyone or practically everyone in the nation. It would obviously not be feasible, if indeed it were possible, to deny the protection provided by the military services, the police, and the courts to those who did not voluntarily pay their share of the costs of government . . . ."); Russell B. Korobkin & Thomas S. Ulen, *Law and Behavioral Science: Removing the Rationality Assumption from Law and Economics*, 88 CALIF. L. REV. 1051, 1139 (2000) (defining a "public good" as "one that exhibits nonrivalrous consumption and for which the costs to suppliers of excluding nonpaying beneficiaries are prohibitively high").

241. *See, e.g.*, Daphne Barak-Erez, *Distributive Justice in National Security Law*, 3 HARV. NAT'L SECURITY J. 283, 285 (2012) (noting the "conventional wisdom that views national security policies as the ultimate example of a 'public good'"); Aziz Z. Huq, *The Social Production of National Security*, 98 CORNELL L. REV. 637, 644 (2013) ("National security has long been understood to be a quintessential public good, one that is uniquely tailored to state monopolization."); Ann R. Markusen, *The Case Against Privatizing National Security*, 16 GOVERNANCE 471, 473 (2003) ("The nature of national security as a public good has been understood for decades and is noncontroversial.").

242. *See supra* notes 165–69 and accompanying text; *see also* WITTES & BLUM, *supra* note 2, at 71 ("[T]he distribution of defensive capacity . . . is a counterweight and a force multiplier for governments that suddenly have to police a proliferation of ultracapable attackers. It offers individuals and companies a potential alternative to government as an address for protection.").

243. *See* Weber, *supra* note 23, at 78 ("[A] state is a human community that (successfully) claims the *monopoly of the legitimate use of physical force* within a given territory. . . . Specifically, . . . the right to use physical force is ascribed to other institutions or to individuals only to the extent to which the state permits it.").

especially independent, of the government "raises big questions about the role and primacy of the state in matters of both national and individual security."[244] Moreover, undermining "[t]he notion that government has a monopoly over security policy . . . erode[s] a part of the conceptual basis for modern government itself."[245] In essence, the impulse to rely on private entities to perform governmental security functions may increase security in the short-term, but undermine security in the long-term by weakening the state, which has long been the locus of national security in the international system.[246]

In other circumstances, however, the government's focus on national security writ large may cause individual insecurity. For example, when the government purchases, but does not disclose, zero-day vulnerabilities in widely used software, it may advance national security writ large (e.g., by using the zero day for espionage), but at the cost of leaving individual and enterprise users vulnerable to exploitation by others who discover the same vulnerability.

As these examples illustrate, in the cybersecurity context, different conceptions of security may be in tension with one another, and security may be very much at odds with other public values.

5. Privacy.—Although not a major focus of existing privatization scholarship, privacy is another value that is especially salient in the cybersecurity realm, particularly in the wake of the disclosures by Edward Snowden.[247] Privacy has inherent importance, but it is also valuable as a

244. WITTES & BLUM, *supra* note 2, at 71; *see* Minow, *supra* note 184, at 1026 ("[T]he expanded governmental use of private military companies erodes the control of force represented by the ascendancy of the nation-state" and "is a symptom of a larger, dangerous challenge to the aspirations of order in the world represented by the system of nation-states and the rule of law.").

245. WITTES & BLUM, *supra* note 2, at 81.

246. *See id.* at 96 ("Today, the modern state appears to be losing its monopoly over violence, if not in principle at least in practice—returning us to a pre-Weberian understanding of the exclusivity of the state as the legitimate purveyor of violence.").

247. Despite its recognized importance, privacy is famously difficult to define. *See, e.g.*, JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 108 (2012) ("There is widespread (though not unanimous) scholarly consensus on the continuing importance of privacy . . . but little consensus about what privacy is or should be."); DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 103 (2008) ("Privacy is too complicated a concept to be boiled down to a single essence."); *id.* at 12–13 (cataloging six conceptions of privacy: (1) "the right to be let alone"; (2) "limited access to the self"; (3) "secrecy—the concealment of certain matters from others"; (4) "control over personal information"; (5) "personhood"; and (6) "intimacy"); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1202 (1998) ("Privacy is a chameleon that shifts meaning depending on context."); Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2087 (2001) ("Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all."). Embracing a "more pluralistic understanding of privacy," Daniel Solove has proposed a typology of sixteen

means of preserving other rights, such as freedom of expression and association.[248] The lack of privacy or fear of surveillance can chill expressive activities.[249]

The importance of both governmental and private actors in the cybersecurity realm brings into sharp relief the question of privacy *from whom*? Individuals—the holders of privacy rights—are typically more concerned about the government accessing their private information than about corporations accessing it.[250] However, concern has grown in recent years about the amount of personal information that corporations aggregate.[251]

Not all cybersecurity efforts implicate individual privacy, but some do. For example, recent legislative debates about the private sector sharing cybersecurity-threat information with the government focused on the risk that individual users' personal information would be shared with government agencies and used for both cybersecurity and criminal-investigation purposes. Privacy advocates strongly opposed information-sharing legislation due to the risks they perceive for individual privacy.[252] The

---

socially recognized privacy problems, grouped under four headings of "information collection," "information processing," "information dissemination," and "invasion." SOLOVE, *supra*, at 10–11, 101; *see also id.* at 101–70 (explaining the typology in detail). Cybersecurity issues may implicate a number of the privacy problems in Solove's typology, including, for example, surveillance, aggregation, identification, insecurity, breach of confidentiality, and disclosure. *See id.* at 106–12, 117–29, 136–46. Moreover, different types of privacy concerns are "not sharply separate," but rather "are functionally interconnected and often simultaneously implicated by the same event or practice." Kang, *supra*, at 1203.

248. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms.").

249. *See* SOLOVE, *supra* note 247, at 108–09 (discussing chilling effects of surveillance); Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1905 (2013) ("[F]reedom from surveillance, whether public or private, is foundational to the practice of informed and reflective citizenship.").

250. This characterization has historically been true of Americans at least. *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1211 (2004) ("Suspicion of the state has always stood at the foundation of American privacy thinking . . . ."); *see also id.* at 1160–64 (contrasting American privacy law's focus on liberty with Europe's focus on dignity).

251. *See, e.g.*, Mary Madden, *Few Feel that the Government or Advertisers Can be Trusted*, PEW RES. CTR. (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/few-feel-that-the-government-or-advertisers-can-be-trusted/ [https://perma.cc/Y2LB-RLHZ] (noting data showing low levels of public trust in both governments and advertisers and increasing levels of concern about information-collection by businesses); Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RES. CTR. (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ [https://perma.cc/8U7Z-AKGJ] (reporting on survey data showing "[w]idespread concern about surveillance by government and businesses"); *cf.* SCHNEIER, *supra* note 144, at 47 ("The overwhelming bulk of surveillance is corporate, and it occurs because we ostensibly agree to it.").

252. *See, e.g.*, Letter from Civil Society Organizations & Security Experts and Academics to Richard Burr, Chairman, Senate Select Comm. on Intelligence, and Diane Feinstein, Vice

privacy concerns would be even more severe if the federal government were to take over private-network defense directly, as General Alexander proposed to U.S. banks.[253]

Consideration of privacy as a public value raises profound questions about the relationship of individuals and their information to both the government and the private sector. In the wake of the Snowden disclosures, many companies have taken a more pro-privacy and thus more adversarial stance vis-à-vis the government.[254] Apple's resistance to government requests for assistance in accessing iPhones is one example.[255] Others include a 2013 lawsuit by Facebook, Microsoft, Google, Yahoo, and LinkedIn that sought the right to disclose information about the number of Foreign Intelligence Surveillance Court orders and National Security Letters the companies receive requesting customer information.[256] More recently, Microsoft challenged and defeated government demands for the content of emails stored in Ireland[257] and sued the Department of Justice to protest gag orders preventing the company from disclosing to customers that the government has sought access to their email.[258]

Despite these recent privacy-protective moves, the private sector is far from a perfect steward of individual privacy rights.[259] At present, there is

---

Chairman, Senate Select Comm. on Intelligence (Mar. 2, 2015), https://www.aclu.org/sites/default/files/field_document/cisa-2015-sign-on-letter.pdf [https://perma.cc/PP2C-4EEH] (objecting to the Cybersecurity Information Sharing Act of 2015 on the grounds that it, among other things, fails to "effectively require private entities to strip out information that identifies a specific person prior to sharing cyber threat indicators with the government").

253. *See supra* notes 142–144 and accompanying text.

254. *See supra* note 144 and accompanying text.

255. *See supra* notes 95–99 and accompanying text.

256. The case triggered a settlement that permits the companies to disclose additional general information about the orders and letters they receive. *See* Devlin Barrett & Danny Yadron, *Government Reaches Deal with Tech Firms on Data Requests*, WALL STREET J. (Jan. 27, 2014), http://www.wsj.com/articles/SB10001424052702303277704579347130452335684 [https://perma.cc/Q8CQ-WMQ8] (explaining that the agreement permits companies to report government requests using numerical ranges of 1,000 or, with additional restrictions, 250); Letter from James M. Cole, Deputy Attorney Gen., U.S. Dep't of Justice, to Colin Stretch, Vice President and Gen. Counsel, Facebook, et al. (Jan. 27, 2014), https://www.justice.gov/iso/opa/resources/366201412716018407143.pdf [https://perma.cc/H474-HB6C] (providing details on new ways in which companies are permitted to report data about requests for customer information).

257. Microsoft Corp. v. United States (In the Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.), 829 F.3d 197, 200–02 (2d Cir. 2016); *see also* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 328–34 (2015) (discussing the Microsoft case and broader issues related to the application of Fourth Amendment rights to data).

258. Complaint for Declaratory Judgment, Microsoft Corp. v. U.S. Dep't of Justice, No. 2:16-cv-00538 (W.D. Wash. Apr. 14, 2016).

259. Megan Graham, *Reminder: Tech Firms Aren't Always the Privacy Advocates We'd Like to Think They Are*, JUST SECURITY (Nov. 1, 2015, 10:32 AM), https://www.justsecurity.org/27257/tech-firms-privacy-advocates/ [https://perma.cc/A4QM-

business value in championing privacy, but in the future, the calculus of business opportunity could shift in a less privacy-protective direction. Determining how to and who can preserve privacy as a public value in the long-term will pose continuing challenges across a range of cybersecurity contexts.

* * *

With the omission of the government's initial gatekeeping role over privatization and the impossibility of using contractual means to restrain private actors, the public-private cybersecurity system poses a more difficult problem than traditional contracting out. And it also implicates a broader range of public law values, making evaluations and tradeoffs to protect such values more complex.

III. Public Law Values in Public-Private Cybersecurity

Although its contours may change, the public-private cybersecurity system will endure in some form for the foreseeable future.[260] Evaluating the extent to which the current public-private cybersecurity system attains or falls short of protecting public law values can suggest ways to "publicize" the system in the short run, as well as illuminate broader lessons for public-private governance of international cybersecurity threats going forward.

Subpart III(A) provides a preliminary assessment of the extent to which the four manifestations of public-private cybersecurity discussed in Part I serve public law values and proposes several remedies for specific public law deficiencies it identifies. Building on this assessment, subpart III(B) then offers more generalizable lessons to shape public-private governance of cybersecurity going forward. In particular, it argues that attempts to protect public law values must not assume that threats to such values are unidirectional. Sometimes the threats to public law values in the cybersecurity context come from the government, not the private sector, which suggests that remedies cannot simply focus, as they have in other contexts, on diffusing government values and processes to private actors. On the other hand, although private parties are now, and will likely remain, crucial to the functioning of the public-private cybersecurity system, their present support of public law values in many contexts may be a fortuity, not a structural feature. Their position may shift over time, creating new challenges to public law values. Finally, the complexities of the public-

---

NU2E] (arguing that when companies stand up for their customers' rights, "companies aren't fighting in *our* best interests, they are fighting to protect theirs").

260. *Cf.* Dickinson, *supra* note 24, at 387 (arguing that "the trend toward outsourcing of foreign affairs functions previously performed by state bureaucracies . . . is probably irreversible. The privatization train has not only already left the station, but has gone far down the track").

private cybersecurity system suggest that the nature of the remedies for public law problems will differ from those in traditional privatization and that remedies in the cybersecurity realm will be highly context dependent.

A. How "Publicized" Is the Current System?

The four manifestations of public-private cybersecurity differ dramatically in the extent to which they support public law values and in the nature and origin of breakdowns when they do not.

1. Botnet Takedowns: Publicly Beneficial Partnerships.—Botnet takedowns present the most positive public law-values story among the cybersecurity scenarios discussed in this Article.[261]

Regardless of whether they are carried out by private actors, the FBI, or private companies and the FBI acting together, the takedowns at least arguably improve security for individual users by disrupting criminal operations. The takedowns have been criticized as engaging in whack-a-mole with cybercriminals who establish new botnets to replace those that are disrupted.[262] But at the same time, reports indicate that at least in the short-term, takedown operations do cause a decrease in criminal activity, thereby improving security.[263]

The fact that botnet takedowns in the United States occur pursuant to federal court orders helps to ensure that they serve additional public law values as well.[264] Court supervision helps to hold those engaging in

---

261. This is not to dismiss interesting questions arising from the substantive merits of the legal theories deployed by both governmental and private actors in support of botnet takedowns. Deputy Attorney General James M. Cole called the government's arguments, at least, "creative lawyering." *See* Cole, *supra* note 49; *infra* notes 268–69 and accompanying text; *cf.* Zeitlin, *supra* note 42 (exploring Fourth Amendment implications of law enforcement botnet takedowns).

262. *See, e.g.*, Fahmida Y. Rashid, *Botnet Takedowns: A Game of Whack-a-Mole?*, PC MAG. (Apr. 3, 2012), http://securitywatch.pcmag.com/security/296250-botnets-takedowns-a-game-of-whack-a-mole [https://perma.cc/N7TB-HED2] (discussing the whack-a-mole argument).

263. *See, e.g.*, Gregg Keizer, *Rustock Take-Down Proves Botnets Can Be Crippled, Says Microsoft*, COMPUTERWORLD (July 5, 2011), http://www.computerworld.com/article/2509934/security0/rustock-take-down-proves-botnets-can-be-crippled—says-microsoft.html?page=2 [https://perma.cc/WC9R-6MYG] (reporting on a significant worldwide drop in spam following the takedown of the Rustock spamming-malware botnet).

264. As implemented in the United States so far, botnet takedowns do not appear to pose a substantial risk to individual privacy, although different implementation mechanisms might raise privacy concerns. The FBI has been careful to note that in taking over botnet command and control infrastructure, it does not "access any information that may be stored on an infected computer." *See* Press Release, U.S. Dep't of Justice, Department of Justice Takes Action to Disable International Botnet (Apr. 13, 2011), https://www.fbi.gov/newhaven/press-releases/2011/nh041311.htm [https://perma.cc/VUN8-ATSZ]. Rather than communicating directly with individual users whose computers are infected, the government and private companies that undertake takedown operations have worked with Internet service providers who communicate with their customers whose computers are infected with the botnet malware. If the government instead were to engage in direct

takedown operations accountable. Before a takedown operation occurs, the government or private actors file legal arguments and factual allegations with a neutral federal judge who independently adjudicates the strength of the claims. The claims are initially judged ex parte and under seal—without notice to the accused bot herders—to avoid giving the bot herders the opportunity to change their operations to avoid the takedown operation. After the takedown, however, the court filings and order are unsealed and posted publicly,[265] resulting in almost complete, if slightly delayed, transparency.

The public posting of the litigation documents reveals not just that a takedown operation has occurred but also who is responsible for the actions. This, in turn, creates the possibility for after-the-fact accountability. At the temporary-restraining-order stage—before botnet operators have been notified and before the takedown occurs—district courts have required Microsoft to post bonds of hundreds of thousands of dollars.[266] Posting of the litigation documents also creates the possibility that if a takedown operation goes awry and harms, for example, a legitimate business, the business could file a lawsuit after the fact.

The litigation-based, court-supervised format of takedown operations also preserves a measure of due process, even for bot herders. The botnet takedowns occur pursuant to temporary restraining orders or preliminary injunctions, and then several months pass between public posting of litigation documents and the courts' entry of final judgment, permanently transferring control of the botnet domains to the government or private company that

---

remediation efforts with respect to infected personal computers, privacy could become a much more significant concern. The Dutch government in the first botnet takedown operation engaged in such action, creating some precedent for direct governmental involvement in remediation. *See Dutch Team Up*, *supra* note 63 (reporting that, with the assistance of a cybersecurity company, the Dutch police "upload[ed] a 'good' bot developed by police" to infected computers, an action that "represents a bold move, as infecting anyone's computer—whether it's with a 'good' bot or a malicious one—is likely against the law in many countries").

265. *See, e.g.*, CITADEL BOTNET, http://www.botnetlegalnotice.com/citadel/# [https://perma.cc/9K5B-S4JX] (providing filings and court orders related to the Citadel botnet takedown); Press Release, U.S. Dep't of Justice, *supra* note 264 (providing links to court documents related to the Coreflood botnet takedown).

266. *See, e.g.*, *Ex Parte* Temporary Restraining Order and Order to Show Cause re Preliminary Injunction at 13, Microsoft Corp. v. John Does 1-8 Controlling a Computer Botnet Thereby Injuring Microsoft and Its Customers, No. A13-cv-1014 (W.D. Tex. Nov. 25, 2013) http://botnetlegalnotice.com/zeroaccess/files/Ex_Parte_TRO.pdf [https://perma.cc/4MTG-MJKH] (ordering Microsoft to post bond of $250,000 with the court as part of the ZeroAccess botnet takedown); *Ex Parte* Temporary Restraining Order and Order to Show Cause re Preliminary Injunction at 19, Microsoft Corp. v. John Does 1-82, No. 3:13-cv-319 (W.D.N.C. May 29, 2013) http://botnetlegalnotice.com/citadel/files/Ex_Parte_TRO.PDF [https://perma.cc/7FGZ-WQA7] (ordering Microsoft to post bond of $300,000 with the court as part of the Citadel botnet takedown).

undertook the takedown.[267] In that time, bot herders (or those erroneously accused of operating botnets) could challenge the takedown.

In addition, recent botnet takedowns show the upside of public-private coordination with respect to fairness in the allocation of resources. Private companies have incentives to target only the botnets that exploit their software. If private companies alone undertook takedown operations, then botnets that lack a clear nexus to a company—or a clear nexus to a *well-resourced* company—might go unaddressed. The government can serve as a helpful backstop, targeting botnets that involve flaws in open-source software or in software not developed by a major company. The private sector in this circumstance serves as a force multiplier, extending botnet fighting resources beyond what the government acting alone might devote.

Among the cybersecurity contexts addressed in this Article, botnet takedowns are the anomalous case because they involve judicial review with opportunities for contestation by those adversely affected and with transparency about what has occurred and who is responsible. Given these circumstances, the fact that botnet takedowns tend to support public values is perhaps not surprising: they occur in the context of a court and litigation system that the United States entrusts with adjudicating contested claims fairly, impartially, and in the service of larger goals of justice. Turning to Article III courts and litigation is not necessarily an option for the other cybersecurity contexts.

Even botnet takedowns, however, raise some concerns. Although there is an opportunity for bot herders to challenge the takedown operations, none have so far done so. Judges have issued final injunctions approving takedowns without the benefit of adversarial testing of either the evidence or legal theories used to justify the takedowns.[268] The takedowns have not resulted in published opinions or review by appellate courts. To remedy some of the procedural oddities of the takedown suits, district court judges might consider appointing an amicus to argue the side of the absent defendants, providing adversarial testing of the government's and private companies' positions.[269]

---

267. For an example, see *supra* notes 45–53 and accompanying text.

268. Moreover, the Obama Administration proposed legislation to more clearly ground its authority to seek botnet-takedown injunctions. *See* Kristen Eichensehr, *White House Cybersecurity Bill: Botnets and "Creative Lawyering,"* JUST SECURITY (Jan. 14, 2015, 11:27 AM), https://www.justsecurity.org/19102/white-house-cybersecurity-bill-botnets-creative-lawyering/ [https://perma.cc/LPU2-LU2U] (discussing the White House's legislative proposal's section on "*Ensuring* Authority for Courts to Shut Down Botnets").

269. Other courts routinely turn to appointed amici to ensure full and adversarial presentation of legal issues. For example, the Supreme Court has a longstanding practice of appointing amici when parties decline to address a particular argument or to defend a case. *See* Neal Devins & Saikrishna B. Prakash, *Reverse Advisory Opinions*, 80 U. CHI. L. REV. 859, 889 (2013) (endorsing appointment of amici in limited circumstances); Amanda Frost, *The Limits of Advocacy*, 59 DUKE

2. Securing Software: Persistent Insecurities & Conflicting Incentives.—No software is perfectly secure, and most software is far from secure. Widespread networking has fostered persistent insecurities that in turn put personal and business information at risk of disclosure.

Insecurity continues at least partly due to competing conceptions of security. Software companies focus on individual or enterprise-level security, seeking to patch vulnerabilities to prevent unauthorized access to systems and networks or unintended functions.[270] On the other hand, the U.S. government is responsible for national security, which can include exploiting individual security vulnerabilities, for example, for foreign espionage.[271] The patching of software that protects individual security can directly impede actions that the government believes serve national security interests. But these differing conceptions are not always in tension. If individual-level vulnerabilities are present in U.S. government or critical infrastructure systems, then individual and national security concerns align in favor of patching vulnerabilities.

Nonetheless, the tension between individual and national security has fostered situations, like the Apple–FBI controversy, in which the private sector—which wants to patch vulnerabilities—is opposed to the U.S. government—which sometimes wants to remedy vulnerabilities but sometimes wants to exploit them. It is therefore useful to consider their approaches to remedying software vulnerabilities separately.

As described in Part I, private companies test their products for vulnerabilities, but in recent years they have increasingly turned to bug bounty programs, wherein they pay researchers who discover flaws in the companies' software.[272] From the perspective of public law values, the bug bounty programs are a positive step. They increase the number of bugs that

---

L.J. 447, 466–67 (2009) (noting examples of the Supreme Court appointing amici); Brian P. Goldman, Note, *Should the Supreme Court Stop Inviting Amici Curiae to Defend Abandoned Lower Court Decisions?*, 63 STAN. L. REV. 907, 912–18 (2011) (providing a history of Supreme Court appointments of amici). The Foreign Intelligence Surveillance Court, which operates ex parte and in secret, now has a system where the court can request amicus service from several preapproved counsel. *See* 50 U.S.C.A. § 1803(i) (West 2015) (authorizing the court to designate individuals to serve as amicus curiae); *Amici Curiae*, U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT, http://www.fisc.uscourts.gov/amici-curiae [https://perma.cc/F9UK-YZV2] (listing "Individuals Designated as Eligible to Serve as an Amicus Curiae Pursuant to 50 U.S.C. § 1803(i)(1)"). Although the federal district court rules of procedure "do not expressly provide for amicus participation . . . district courts enjoy wide discretion to invite such participation." Brianne J. Gorod, *The Adversarial Myth: Appellate Court Extra-Record Factfinding*, 61 DUKE L.J. 1, 22 (2011).

270. *See supra* note 65 and accompanying text.

271. *See* Daniel, *supra* note 86 (discussing the tradeoff between disclosure and exploitation of vulnerabilities).

272. *See supra* notes 90–94 and accompanying text.

are remedied (improving security) and thereby decrease the risks of compromises that infringe users' privacy.

The problem with bug bounty programs is that they are insufficient. Not all companies offer bounty programs.[273] Even companies that do cannot necessarily compete with prices that bugs can fetch on the black market, where governments, including the United States, have reportedly driven up prices.[274]

The role of the U.S. government with respect to software vulnerabilities is more problematic from a public law-values perspective. The government's decisions to purchase vulnerabilities on the black market, stockpile them, and exploit flaws in software of U.S. companies all challenge public law values. Government purchases of black-market vulnerabilities bid up prices and hamper companies' ability to compete monetarily with their bug bounty programs.[275] Government exploitation of vulnerabilities in U.S. companies' software—when the exploitation is revealed—fosters the perception not just that the companies' products are insecure but also that the company may be complicit in the U.S. government's actions, and thus untrustworthy for purchasers in foreign markets.[276] To its credit, the White House has released some information about the vulnerability equities process that it uses to decide whether and when to disclose vulnerabilities to software makers.[277] But the extent of the information that can be released is necessarily limited by the demands of national security, including, for example, the need to avoid alerting espionage targets of how the United States is spying. The lack of transparency about operations also limits the government's accountability for the decisions it makes and prevents informed public debate about whether the government is striking the appropriate balance between individual and national security.

Within the limits of necessary secrecy and consistent with national security, the government could take several actions to shift the balance in

---

273. Until recently, Apple was the most prominent example of a company that lacked a bounty program. *See* Nicole Perlroth & Katie Benner, *Apple Policy on Bugs May Explain Why Hackers Would Help F.B.I.*, N.Y. TIMES (Mar. 22, 2016), http://www.nytimes.com/2016/03/23/technology/apple-policy-on-bugs-may-explain-why-hackers-might-help-fbi.html [https://perma.cc/HFF2-FYZL] (reporting speculation that Apple's lack of a bounty program may have made hackers more willing to assist the FBI in the San Bernardino case). Apple announced that it would commence a bounty program in September 2016 with potential payouts up to $200,000. Lily Hay Newman, *Apple's Finally Offering Bug Bounties—with the Highest Rewards Ever*, WIRED (Aug. 4, 2016), https://www.wired.com/2016/08/apples-finally-offering-bug-bounties-highest-rewards-ever/ [https://perma.cc/8VFJ-3YRA].

274. *See supra* note 94 and accompanying text.

275. *See supra* note 94 and accompanying text.

276. *See infra* note 281 and accompanying text.

277. *See supra* notes 86–88 and accompanying text.

favor of individual security, supporting or complementing private sector efforts to better secure software.

First, the government could provide some public funding for certain bug bounty programs. Public funding could help to stimulate bug hunters to target software that is particularly important, for example, to critical infrastructure. It might also be used to support bounties for bugs in open-source software, which is not the responsibility of any particular company. Private companies have taken some steps to support bounty programs for open-source software,[278] but public funding could substantially increase incentives for bug hunters to address open-source-software flaws, which, as recent examples have shown, can be important and pervasive.[279]

Second, to address due process or fairness concerns with the U.S. government deciding to impose a risk of harm on U.S. companies by exploiting flaws in the companies' software, the government could publicly pledge not to exploit flaws in U.S. companies' software in offensive operations.[280] The ubiquity of some U.S. companies' software around the world suggests that such a pledge might be costly to the U.S. government, which would have a more limited range of options for exploitable software. Such a pledge, however, could help to repair the relationships between the U.S. government and U.S. technology companies that suffered serious damage as a result of the Snowden disclosures and more recently lined up with Apple against the government's demand that the company bypass

278. *See, e.g.*, Nicole Perlroth, *Hacking for Security, and Getting Paid For It*, N.Y. TIMES (Oct. 14, 2015), http://bits.blogs.nytimes.com/2015/10/14/hacking-for-security-and-getting-paid-for-it/?_r=0 [https://perma.cc/P8V4-WPUE] (reporting that after the discovery of the Heartbleed bug, "the nonprofit Linux Foundation and more than a dozen major tech companies started an initiative to pay for security audits in widely used open-source software"); Michal Zalewski, *Going Beyond Vulnerability Rewards*, GOOGLE (Oct. 9, 2013), https://googleonlinesecurity.blogspot.com/2013/10/going-beyond-vulnerability-rewards.html [https://perma.cc/5TX8-YA69] (announcing that Google will pay for "down-to-earth, proactive improvements" to open-source software).

279. *See* Nicole Perlroth, *Security Experts Expect 'Shellshock' Software Bug in Bash to Be Significant*, N.Y. TIMES (Sept. 25, 2014), http://www.nytimes.com/2014/09/26/technology/security-experts-expect-shellshock-software-bug-to-be-significant.html?_r=0 [https://perma.cc/CUR3-BZF6] (noting that the Shellshock bug in open-source software "can be used to take over the entire machine" and "was not discovered for 22 years"); Bruce Schneier, *Heartbleed*, SCHNEIER ON SECURITY (Apr. 9, 2014, 5:03 AM), https://www.schneier.com/blog/archives/2014/04/heartbleed.html [https://perma.cc/S36A-QV6P] (describing Heartbleed as "a catastrophic bug in Open SSL").

280. *See, e.g.*, ZETTER, *supra* note 72, at 393 (discussing the doctrine of "operational use," whereby "[U.S.] intelligence agencies can't do things that might put [U.S.] businesses at risk unless they have high-level legal authorities sign off on the operation and the company consents"). For example, intelligence agencies cannot "make IBM an unwitting CIA accomplice by having an agent pose as an IBM employee without informing someone at the company who has fiduciary responsibilities." *Id.*

iPhone security features.[281] Relatedly, the cost of the pledge could decrease over time. The Snowden disclosures prompted a number of countries to focus on developing domestic software and technologies and turning away from U.S. products,[282] a move that could increase the targets that would be breachable without exploiting vulnerabilities in U.S. companies' software.

Finally, the U.S. government could increase the extent to which it purchases vulnerabilities and discloses them to software makers for patching. The government does this in some circumstances, as evidenced by White House Cybersecurity Coordinator Michael Daniel's explanation of the vulnerability equities process,[283] but the relative frequency with which it purchases and discloses is unclear.[284] It is also unclear whether or how often the government purchases vulnerabilities for the sole purpose of disclosing and patching, as opposed to exploiting and then disclosing.[285] Publicly announcing a policy of increased disclosure could improve relations with U.S. technology companies and improve the security of products used by many individuals in the United States, making U.S. companies both more competitive and perhaps more willing to assist the government in future cases.

3. Publicly Attributing State-Sponsored Intrusions: Increased Transparency, but Accountability Confusion.—The reports prepared by cybersecurity companies attributing intrusions to state-sponsored threat

281. *See, e.g.*, Ellen Nakashima, *Google, Facebook and Other Powerful Tech Firms Filing Briefs to Support Apple*, WASH. POST (Feb. 28, 2016), https://www.washingtonpost.com/world/national-security/google-facebook-and-other-powerful-tech-firms-filing-briefs-to-support-apple/2016/02/28/beb05460-de48-11e5-846c-10191d1fc4ec_story.html [https://perma.cc/ETC6-RVLG] (detailing technology companies' support for Apple's position in the San Bernardino case); Gerry Smith, *'Snowden Effect' Threatens U.S. Tech Industry's Global Ambitions*, WORLD POST (Jan. 24, 2014), http://www.huffingtonpost.com/2014/01/24/edward-snowden-tech-industry_n_4596162.html [https://perma.cc/7NJ8-JU2S] (reporting that U.S. cloud-services providers may "lose as much as $35 billion over the next three years as fears over U.S. government surveillance prompt foreign customers to transfer their data to cloud companies in other countries").

282. *See, e.g.*, Arne Delfs & Tony Czuczka, *Merkel Urges European Internet Push to Blunt U.S. Surveillance*, BLOOMBERG (July 19, 2013), http://www.bloomberg.com/news/articles/2013-07-19/merkel-urges-european-internet-push-to-blunt-u-s-surveillance [https://perma.cc/WP3V-VFBE] (reporting on German Chancellor Angela Merkel's suggestion that "Europe should promote home-grown Internet companies to avoid U.S. surveillance" and other German lawmakers' advocating for development of European rivals to Google and Facebook).

283. *See supra* notes 86–88 and accompanying text.

284. *See supra* note 87. To increase the legitimacy of the vulnerability equities process, the White House could also release reports detailing the number of vulnerabilities considered each year and the number disclosed to software vendors. Alex Grigsby, *Making Sense of the U.S. Policy on Disclosing Computer Vulnerabilities*, COUNCIL ON FOREIGN REL. (Sept. 22, 2015), http://blogs.cfr.org/cyber/2015/09/22/making-sense-of-the-u-s-policy-on-disclosing-computer-vulnerabilities/ [https://perma.cc/M4C8-LJJE].

285. *See supra* note 171.

actors improve transparency and security, but create accountability confusion and possibly due process and fairness concerns.

As discussed in Part I, the Mandiant report identifying PLA Unit 61398 provided a publicly citable source attributing intrusions to the Chinese government and thereby increased transparency regarding the threats to U.S. businesses and other entities. Subsequent reports have done the same with respect to other government actors.[286] The reports often include some threat indicators that can be used to better secure systems and networks against intrusions, which improves security.[287]

On the other hand, the reports foster confusion about accountability for decisions with potentially significant foreign-relations consequences. The companies making the accusations against foreign governments are not formally accountable for the foreign-relations fallout from the substance and timing of their accusations. A company could decide to release a report at a politically sensitive time, causing harm to the government's foreign-relations priorities. The company does not bear the cost of foreign-relations harms, but the federal government, which would bear such costs, is not responsible for the company's decision to launch the accusation. In other circumstances, the government may support or condone private actors' accusations precisely to avoid accountability for making the accusation itself.

The relationship between the private company's accusation and the federal government is often murky. How is a foreign country to know whether the U.S. government was blindsided by the report or instead fed information to the company? Foreign governments may assume that private attributions are driven by the federal government and hold the government accountable for private actors' conduct.

While accountability for the consequences of reports attributing state-sponsored attacks is unclear, there may be somewhat more accountability with respect to the substance and accuracy of accusations. Public release of the reports opens the attribution determination and the evidence to challenge by the U.S. government, foreign governments (including the accused government), or competitor cybersecurity firms. Consider the Russian government-sponsored hack of the Democratic National Committee.[288] After CrowdStrike accused the Russian government of involvement, other cybersecurity firms reviewed the evidence and confirmed CrowdStrike's

286. *See supra* note 118.

287. *See, e.g.*, MANDIANT, *supra* note 109, at apps. C–G.

288. *See* Ellen Nakashima, *Russian Government Hackers Penetrated DNC, Stole Opposition Research on Trump*, WASH. POST (June 14, 2016), https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html [https://perma.cc/6PMU-HTGG].

conclusions.[289] Moreover, the existence of sophisticated private sector attribution capabilities may hold the U.S. government more accountable for accusations it makes against foreign governments as well.[290] Private actors challenged the FBI's attribution of the Sony hack to North Korea,[291] and the government should expect similar questioning from the private sector with respect to future allegations against foreign governments.

The private cybersecurity reports may also create due process and privacy concerns. Some of the reports have included highly specific attribution to individuals.[292] Links to particular individuals are, on the one hand, impressive and key to tying intrusions to state actors. In some reports, individuals' interactions with, for example, email and social media sites reveal links between the individual and an intrusion, and the individual is then identified as an employee of a state organization—transitively linking the foreign government to the intrusion.[293] On the other hand, the highly personal nature of some of the attributions is itself intrusive from the perspective of the individual, who suddenly finds his or her photos, home address, family details, license plate, and social media information publicly

289. *See, e.g.*, Patrick Tucker, *How Putin Weaponized Wikileaks to Influence the Election of an American President*, DEFENSE ONE (July 24, 2016), http://www.defenseone.com/technology/2016/07/how-putin-weaponized-wikileaks-influence-election-american-president/130163/ [https://perma.cc/HV74-H28W] (discussing confirmation of CrowdStrike's conclusion by other companies).

290. Microsoft recently proposed the establishment of an international organization, modeled on the International Atomic Energy Agency, that would review evidence and make attribution determinations for attacks carried out by nation-states. CHARNEY ET AL., *supra* note 4, at 11–12. Microsoft suggests that the organization, which would draw technical experts from government, the private sector, academia, and civil society, could provide "peer review" of reports attributing attacks to governments, thereby "improving the quality of the results." *Id.*; *see* Herb Lin, *Microsoft Proposes an Independent Body for Making Attribution Judgments*, LAWFARE (June 24, 2016), https://www.lawfareblog.com/microsoft-proposes-independent-body-making-attribution-judgments [https://perma.cc/6WVB-JKHE] (noting that if the proposed organization were feasible, "it would help to a considerable extent address the politicization of many attribution judgments today").

291. *See, e.g.*, Kim Zetter, *Critics Say New Evidence Linking North Korea to the Sony Hack Is* Still *Flimsy*, WIRED (Jan. 8, 2015), http://www.wired.com/2015/01/critics-say-new-north-korea-evidence-sony-still-flimsy/ [https://perma.cc/Y22G-CRC8] (discussing questioning of U.S. government attribution of the Sony hack to North Korea).

292. *See, e.g.*, MANDIANT, *supra* note 109, at 52–55 (profiling Wang Dong); THREATCONNECT & DEFENSE GROUP INC., CAMERASHY: CLOSING THE APERTURE ON CHINA'S UNIT 78020, at 5, 35–53 (2015), http://cdn2.hubspot.net/hubfs/454298/Project_CAMERASHY_ThreatConnect_Copyright 2015.pdf?t=1443030820943&submissionGuid=8b242912-4426-45ef-ba7f-2441ab220cb5 [https://perma.cc/DH2H-D8BG] (identifying Chinese PLA Unit 78020 as responsible for espionage against Southeast Asian targets, particularly related to the South China Sea, and profiling PLA officer Ge Xing).

293. *See, e.g.*, THREATCONNECT & DEFENSE GROUP INC., *supra* note 292, at 35–53 (identifying PLA officer Ge Xing based in part on, for example, his QQ Weibo account).

revealed,[294] and covered in the international media.[295] Such individuals have no clear recourse against companies that choose to publicize the individuals' names and information. One hopes that the companies act responsibly and accuse individuals only with very strong and corroborated evidence, but the fact remains that private companies, not government officials, are making decisions to target particular individuals. Unlike botnet takedowns, these accusations do not proceed in court; they are adjudicated, if at all, in the court of public opinion and with little or no regard for possible harm to the individuals involved.

Accusations may effectively be transferred into court if the government becomes involved. In May 2014, the United States indicted an individual initially named in the Mandiant report for breaches of U.S. companies.[296] The indictment brings the possibility of severe criminal penalties, but it also provides an opportunity to contest the accusations and assurance that the decision to target the individual proceeded through government channels that are structurally designed to balance public law values (though many would argue that they do not always succeed in striking a proper balance).

Naming of individuals as intrusion perpetrators may help to deter not just the named individual but others in his or her country from engaging in behavior that might spark a future report. But that deterrence comes at the possible cost of due process and privacy protections for individuals whose rights are weighed, if at all, by private actors that have incentives to demonstrate their attribution prowess by naming names and posting photos.

4. Defending Private Networks: Security & Public Values Compromises.—Private systems and networks in the United States are not secure.[297] Frequent headlines make plain the persistent lack of security

294. *See, e.g.*, *id.* (detailing identifying information about PLA officer Ge Xing, including his home address, car license plate, bike riding routes, and (partially redacted) photos of his child).

295. *See, e.g.*, Josh Chin, *Cyber Sleuths Track Hacker to China's Military*, WALL STREET J. (Sept. 23, 2015), http://www.wsj.com/articles/cyber-sleuths-track-hacker-to-chinas-military-1443042030 [https://perma.cc/7JU8-3NPC] (covering the ThreatConnect report and discussing Ge Xing); Josh Harkinson, *Meet the 3 Chinese Hackers Pwned by Mandiant*, MOTHER JONES (Feb. 19, 2013), http://www.motherjones.com/mojo/2013/02/chinese-hackers-pwned-mandiant-cyber-attack-new-york-times [https://perma.cc/U8YP-BHDE] (reporting on the Mandiant report).

296. *Compare* Indictment, United States v. Wang Dong et al., No. 14-118 (W.D. Pa. May 1, 2014), http://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf [https://perma.cc/4YSD-ZJYM] (charging Wang Dong with violating, inter alia, the Computer Fraud and Abuse Act), *with* MANDIANT, *supra* note 109, at 52–55 (profiling Wang Dong).

297. Neither, of course, are government networks. *See, e.g.*, David Alexander, *The OPM Hack Was a Lot Worse than Previously Disclosed*, HUFFINGTON POST (Sept. 23, 2015), http://www.huffingtonpost.com/entry/opm-hack_5602f64be4b08820d91b59c2 [https://perma.cc/DB3A-D2YR] (reporting that the hack of the Office of Personnel Management compromised the personal information of 21.5 million people, including the fingerprints of 5.6 million people); Cory Bennett, *Pentagon Restores Hacked Network*, THE HILL (Aug. 10, 2015),

among private sector systems and risks to personal privacy due to compromised personal information, such as health records.[298] Currently the private sector is somewhat transparent about some security problems. Regulations applicable to some sectors require companies to disclose compromises to government officials,[299] state data-breach laws require businesses to notify individuals' whose personal information is compromised,[300] and Securities and Exchange Commission guidance instructs public companies to disclose material breaches.[301] Private actors are also somewhat accountable for some security breaches, and perhaps increasingly so. Companies routinely settle cases stemming from breaches of personal information and brought pursuant to state data-breach-notification laws, and one court of appeals has allowed class actions to proceed based on the likelihood of harm to individuals from retailers' data breaches.[302] In another case stemming from a breach of personal information, a different circuit court recently upheld the Federal Trade Commission's authority to bring cases against companies for unfair and deceptive consumer

---

http://thehill.com/policy/cybersecurity/250730-pentagon-restores-hacked-email-system [https://perma.cc/W38V-D9LT] (discussing Russian hackers' compromise of the Joint Chiefs of Staff's unclassified email system); Michael S. Schmidt & David E. Sanger, *Russian Hackers Read Obama's Unclassified Emails, Officials Say*, N.Y. TIMES (Apr. 25, 2015), http://www.nytimes.com/2015/04/26/us/russian-hackers-read-obamas-unclassified-emails-officials-say.html [https://perma.cc/2S7U-K34J] (discussing Russian hackers' intrusions into the White House, State Department, and Defense Department).

298. *See, e.g.*, Jim Finkle, *Premera Blue Cross Hacked, Medical Information of 11 Million Customers Exposed*, HUFFINGTON POST (Mar. 17, 2015), http://www.huffingtonpost.com/2015/03/17/premera-blue-cross-cybera_n_6890194.html [https://perma.cc/98LZ-EHFZ] (reporting on compromise of data, including claims data and "clinical information," for 11 million customers of Premera Blue Cross, a health insurance company).

299. *See* NRC Cyber Security Event Notifications, 10 C.F.R. § 73.77(a)(3) (2016) (requiring licensees who operate nuclear power plants to notify the Nuclear Regulatory Commission of suspected or actual cyber attacks and of activities that "may indicate intelligence gathering or pre-operational planning related to a cyber attack"); DoD Mandatory Cyber Incident Reporting Procedures, 32 C.F.R. § 236.4(b) (2016) (requiring Defense Department contractors to report certain "cyber incidents" that affect the contractors' systems or defense information in their possession or that "affect[] the contractor's ability to provide operationally critical support").

300. *See, e.g.*, *Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (Jan. 4, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/4MK5-2BT3] (compiling data-breach laws from forty-seven states and several U.S. territories).

301. *CF Disclosure Guidance: Topic No. 2: Cybersecurity*, U.S. SEC. & EXCHANGE COMM'N (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm [https://perma.cc/Y3C5-Y9ZJ].

302. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (finding standing for data-breach victims based on an "objectively reasonable likelihood" of injury such as identity theft or credit-card fraud); *see also* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 966–70 (7th Cir. 2016) (concluding that data-breach plaintiffs "have alleged enough to support Article III standing").

practices, including failure to take reasonable measures to secure customers' personal data.[303]

These developments suggest a shift toward greater accountability for companies that fail to secure personal information, and relatedly, increased due process for victims of data breaches. They do little, however, to settle broader debates about the responsibility for protecting against other types of threats—including theft of intellectual property and compromises of critical infrastructure systems—and other types of actors, especially foreign government or government-affiliated attackers. In fact, in ruling against companies that suffered customer data breaches, the courts of appeals have implicitly relied on the fact that the companies were compromised by cybercriminals, not nation-states.[304]

Should the rules be different for nation-state threats? In the physical world, companies are expected to take reasonable measures to protect themselves against ordinary crime—locks on doors, surveillance cameras, alarm systems, security guards, etc. They are not, however, expected to defend against missiles launched by foreign militaries; that is the responsibility of the government. Yet, in the cybersecurity sphere, the government has disclaimed primary responsibility for defending the private sector against even foreign-government intrusions, placing that duty solidly on private entities, with assistance in the form of some information sharing. So far, this system is failing to provide adequate security. Although some companies may be sufficiently sophisticated to grapple with nation-state-based threats,[305] most—including many critical-infrastructure entities—are not.

The obvious alternative to making private entities responsible for defending themselves against even foreign government attacks is to make the U.S. government responsible for defending them. Even if that were possible—a dubious assumption given the government's apparent inability to secure its own systems—the government protection model would raise different public law-values issues, chiefly privacy concerns. Take the suggestion that the NSA should have direct access to banks' networks,[306] or consider direct intelligence community access to telecommunications

303. Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 359 (3rd Cir. 2015).

304. In upholding the Federal Trade Commission's authority to bring an enforcement action against Wyndham Hotels for unfair or deceptive practices, the Third Circuit rejected the hotel's argument that it should not be held liable for failing to secure customers' information "when the business *itself* is victimized by criminals." *Id.* at 246 (quoting Wyndham's Brief); *see also Remijas*, 794 F.3d at 693 (holding that plaintiffs have shown a "substantial risk of harm" from breach of a customer data because "[w]hy else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities").

305. *See supra* notes 153–60 and accompanying text.

306. *See supra* note 143 and accompanying text.

companies' networks. Making the government directly responsible for defending such private networks would subject vast amounts of individual and corporate data to government scrutiny and the possibility of use for purposes far afield of the cybersecurity rationale for which access was granted.

The current system of private defense against foreign government threats seems worryingly insufficient. Private actors—and potentially important ones—will lose against attacks by foreign states, but the alternative of turning private-network defense over to the U.S. government—even if doing so were feasible—comes with different problems. The lack of an obviously preferable alternative suggests that the current system is likely to endure until an external shock changes the balance of concerns. For example, imagine that a foreign government or nonstate terrorist group eventually takes down the electricity grid in a major city,[307] or disables a U.S. stock exchange. In the wake of such an incident and attribution to a foreign actor, governmental attempts to blame the private sector victim for failing to defend itself may ring hollow and force more creative approaches to solving persistent security problems.

B. Promoting Public Law Values in Public-Private Cybersecurity

This preliminary evaluation of how public law values are faring with respect to botnet takedowns, securing software, attribution of state-sponsored intrusions, and defense of private networks reveals several important lessons for cybersecurity in particular and for theories of privatization more broadly.

First, public-private cybersecurity shows that, in the context of complicated public and private roles, concerns about public law values are not unidirectional. Both public law concerns and solutions can come from multiple and sometimes surprising directions. Unlike traditional privatization, this is not a circumstance where the challenge is simply how to transfer governmental values to the private sector and rein in wayward contractors. In cybersecurity, sometimes the government itself threatens public law values. Other times, the government is simply absent. In those circumstances, the private sector may step in, acting in ways that bolster public values.[308]

---

307. *Cf.* Ellen Nakashima, *Russian Hackers Suspected in Attack that Blacked Out Parts of Ukraine*, WASH. POST (Jan. 5, 2016), https://www.washingtonpost.com/world/national-security/russian-hackers-suspected-in-attack-that-blacked-out-parts-of-ukraine/2016/01/05/4056a4dc-b3de-11e5-a842-0feb51d1d124_story.html [https://perma.cc/SW8R-QXDA].

308. For example, private companies' public attributions of state-sponsored cyberattacks may become increasingly important during the Trump Administration. President Trump repeatedly declined to accept the intelligence community's and private companies' attribution of the DNC hack to Russia. *Compare* Press Release, Office of the Dir. of Nat'l Intelligence, Joint Statement from the Dep't of Homeland Sec. & Office of the Dir. of Nat'l Intelligence on Election Sec. (Oct. 7,

Second, empowered private parties are crucial to how the public-private cybersecurity system is currently functioning. So far, the role of private parties is in many ways a positive story. In the absence of government action, private companies have used innovative legal strategies to address the problem of botnets, and they created bug bounty programs to better secure their software. When the government's hands were tied by limitations on disclosing classified information, companies published detailed reports that increased transparency about the source of state-sponsored intrusions into U.S. companies. But in each of these circumstances and in others where private parties have played a so far constructive role, they have had business reasons for taking action—for example, avoiding public relations harms from misuse or exploitation of their products, or advertising their capabilities to attract new clients.

As a general matter, private interests are often at odds with public law values—the concern that has spurred traditional privatization literature—and the fortuitous alignment in the cybersecurity sphere is unlikely to be permanent or total. The first step to guarding against possible future shifts in the alignment between private interests and public law values may be, as this Article aims to do, increasing understanding and awareness of the quasi-governmental role that private parties are playing in cybersecurity. In addition, representatives of technology and cybersecurity companies routinely testify before Congress on cybersecurity-policy issues.[309] Such hearings often focus on the companies' views about the actions of the government, but they should also address the role of the companies

---

2016), https://www.dni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1423-joint-dhs-odni-election-security-statement [https://perma.cc/9XX2-NRYD] ("The U.S. Intelligence Community . . . is confident that the Russian Government directed the recent compromises of e-mails from [U.S.] persons and institutions, including [U.S.] political organizations."), *and* Alperovitch, *supra* note 118 (identifying two Russian-government linked hacking groups as responsible for the intrusions at the DNC), *with Donald Trump on Russia, Advice from Barack Obama and How He Will Lead*, TIME (Dec. 7, 2016), http://time.com/4591183/time-person-of-the-year-2016-donald-trump-interview/ [https://perma.cc/3JEJ-ZAMD] (reporting that when asked about Russia's interference in the U.S. election, Trump said, "It could be Russia. And it could be China. And it could be some guy in his home in New Jersey."). If the Trump Administration does not attribute cyberattacks to foreign governments, private companies' attribution reports—though they raise some concerns, as discussed above—could help to fill a transparency gap and potentially serve security interests by naming and shaming attackers.

309. *See, e.g.*, *Outside Perspectives on the Department of Defense Cyber Strategy: Hearing Before Subcomm. on Emerging Threats & Capabilities of the H. Armed Servs. Comm.*, 114th Cong. (2015), http://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=103985 [https://perma.cc/2846-VYKJ] (listing witnesses from, inter alia, FireEye and VMWare); *Protecting America from Cyber Attacks: The Importance of Information Sharing: Hearing Before S. Comm. on Homeland Sec. & Governmental Affairs*, 114th Cong. (2015), http://www.hsgac.senate.gov/hearings/protecting-america-from-cyber-attacks-the-importance-of-information-sharing [https://perma.cc/UV2A-J2LC] (listing witnesses from, inter alia, American Express, Microsoft, and FireEye).

themselves. Congress could ask company representatives questions about, for example, how the companies consider foreign-relations consequences of their actions or what measures the companies take to protect against possible negative consequences of actions like botnet takedowns. Increasing discussion would bring additional attention to and understanding about the actions that companies are currently undertaking and about their role vis-à-vis the U.S. government.

Third, as discussed in subpart II(A), the nature of the public-private cybersecurity system changes the nature of possible remedies to public law-values concerns. The conventional solution of baking public law values into the contractual requirements for government contractors is not available in the cybersecurity context and, moreover, would not necessarily be responsive to the nature of the dangers to public law values. Remedies for concerns about public law values in cybersecurity will be highly context dependent. Although the purpose of this Article is not to resolve every possible public law-values threat, the preceding Parts provide a few examples of context-specific solutions, including court-appointed amici in botnet takedown cases,[310] publicly funded bug bounties for open-source software,[311] and a pledge by the U.S. government not to exploit vulnerabilities in the software of U.S. companies for offensive operations.[312]

The public-private cybersecurity system does not work like the government-driven, top-down models of privatization that have dominated the last few decades. It raises some of the same concerns for public law values, but at the same time, its complexity demands greater vigilance directed at a broader range of actors and greater creativity in remedying problems that do arise.

Conclusion

This Article diagnoses the underappreciated system of public-private governance that has emerged to address U.S. cybersecurity problems in recent years.[313] In the contexts described in Part I, the private sector has come to play a very government-like role, sometimes in conjunction with a less government-like role for the U.S. government. These role inversions are made possible in part by informal partnerships between the private sector and the government and by even less direct, mutually beneficial pursuit of interests by both the private sector and the government with minimal

310. *See supra* notes 268–69 and accompanying text.

311. *See supra* section III(A)(2).

312. *See supra* section III(A)(2).

313. This project focuses nearly exclusively on the United States. There may be valuable insights to be gleaned from comparative study of how other countries are organizing to address cybersecurity.

coordination, but perhaps with some mutual encouragement. As the operation of government-like power becomes more diffuse and more complicated, the actions of private sector actors can implicate the public law values that traditionally apply to governmental actions, and governmental actions may come into increasing tension with public law values.

The public-private cybersecurity system challenges and complicates existing scholarly accounts of privatization. As a procedural matter, in the cybersecurity space, the government does not decide which functions private actors may or should perform; private actors decide for themselves what actions to undertake. The public-private relationships do not operate via contract, thereby eliminating the procedural vehicle scholars have favored for imposing substantive restrictions on privatized activities and the mechanism by which the government reconsiders the allocation of responsibilities to the private sector. As a substantive matter, the cybersecurity context requires a fuller account of public values. The traditional focus on accountability, and secondarily transparency and due process, should be expanded to include provision of security and preservation of privacy. The salience of these values for individuals—the "public" in "public law" values—increases in the cybersecurity context where lack of security is not just a national-level metric, but also a personal experience of insecurity that can lead to identity theft, fraud, extortion, and data loss.

Taken as a whole, the case studies set out above show that the de facto public-private cybersecurity system poses public law challenges that are different from and harder than traditional privatization of government functions. Traditional privatization sparked questions about how to "publicize" private actors—how to make private actors subject to the public law-values requirements that the government abided by when delivering the service at issue prior to contracting out. In other words, traditional privatization raised questions about how to make the private sector more like the government with respect to the values applied to it. In public-private cybersecurity, by contrast, a persistent theme in the contexts described in this Article is that the private sector is already playing a helpful role in protecting public values. The private sector is starting out "publicized." The role of the government, however, is sometimes more questionable, such as when it withholds knowledge of software vulnerabilities, preventing them from being patched, or when it outsources attribution of state-sponsored intrusions to private actors, potentially to avoid accountability for making an accusation. However, while the private sector has played and continues to play a useful role in fostering public values in the contexts discussed in Part I, the private

sector is a fickle guardian of public values, and business imperatives will not always align with public values.[314]

There is no silver-bullet solution to concerns about public law values in cybersecurity. The government and private sector roles and relationships are complicated and shift in different contexts. In this circumstance, the best approach is to focus, as Part III does, on proposals that preserve or strengthen particular public law values in specific circumstances. Such corrections will be necessary in instances where either the private sector or the government has incentives that point away from serving public law values, and they will be particularly crucial in instances where *neither* the private sector nor the government are properly incentivized to protect public values.

Protecting public law values first requires understanding that they may be at risk. This Article has taken a first step by describing the public-private cybersecurity system, identifying relevant public law values, diagnosing risks to public law values in cybersecurity, and proposing lessons for approaching public law-values concerns in cybersecurity going forward. New roles and contexts will continue to evolve and so too must the tools for protecting public values.

314. *Cf.* SCHNEIER, *supra* note 144, at 209 ("Corporate interests may temporarily overlap with their users' privacy interests, but they're not permanently aligned.").