# Cyber Checks and Balances

Elad D. Gil†

How does the digital era affect the ability of governments to "govern"? On the one hand, global connectivity and data-driven technologies provide governments with powerful new ways to exercise coercion. Digital surveillance, content takedowns (i.e., censorship), forced data "localization," and hacking, to take a few examples, have become widely adopted techniques in the toolkits of many democratic states. These techniques enable encroachments on liberty that only two decades ago would seem unthinkable. On the other hand, the exclusive status of the state as "the sovereign" is challenged in cyberspace more than in any other arena by a variety of non-state actors, as well as foreign states. Scholarly accounts accordingly split between two narratives: some scholars view the digital era as the beginning of an era of awesome state power, while others see signs of state decline.

This Article challenges both narratives, arguing that "government power" in cyberspace cannot be theorized as a static concept. Rather, it is determined by a web of interactions with and pressures from forces and actors that, although operating outside the constitutional structure, are akin in their effect to constitutional checks and balances. The Article conceptualizes the cyber checks and balances ecosystem, identifies and analyzes its four principal components—the private sector, the "architecture" of cyberspace, international law, and international politics—and examines the interwoven effects. It demonstrates how cyber checks and balances constrain the government in some ways but empower it in others, sometimes even enabling the government to circumvent legal limitations on its own authority. After mapping this ecosystem, the Article assesses its normative implications. Viewing the balance of power between the state and other forces in cyberspace as a system of checks and balances affords a more accurate and nuanced analysis of governmental exercises of power in the digital domain. More importantly, this Article shows that understanding how this ecosystem is shaping state power can help the traditional forces within the constitutional system—lawmakers, judges, and executive gatekeepers—optimize their checking and balancing, ensuring that government power in cyberspace is exercised effectively yet responsibly.

---

† Post-doctorate research fellow, Hebrew University, Faculty of Law, and the Federmann Cybersecurity Centre; Research fellow, Duke University I&E Initiative. For helpful comments and suggestions, I am grateful to Stuart Barr, Jeff Kosseff, Asaf Lubin, Nadiv Mordechai, Madeline Morris, Yuval Shany, Ori Sharon, Yahli Shershevsky, and participants at the 2020 Cybersecurity Law and Policy Scholars Conference, the Federmann Cybersecurity Centre workshop, the Duke I&E Research Brown Bag workshop, and the College of Management Law School faculty seminar. Thanks also to Aaron Boujenah for excellent research assistance.

54 Cornell Int'l L.J. 381 (2021)

## Introduction

On August 13, 2016, a mysterious group of hackers called "the Shadow Brokers" tweeted the world that it had hacked the National Security Agency (NSA) and stolen many of the agency's most secret and destructive cyberweapons.[1] To add insult to injury, the group put the stolen codes up for auction and taunted the NSA to participate in the bidding.[2] Months later, frustrated with the slow volume of offers and meager media coverage, the group released a trove of NSA hacking tools for free.[3] Predictably, hackers from around the world, some of them state-backed, quickly took advantage and turned these ready-to-use cyberweapons against public and private targets in the United States, as well as on millions of internet users

1. The original Tweeter account @shadowbrokers is no longer active. The full text of the original tweet and linked message is archived at https://github.com/samgranger/EQGRP.

2. *Id.* (the message reads "Q: What is in auction files? A: Is secret. Equation Group [i.e., the NSA] not know what lost. We want Equation Group to bid so we keep secret. You bid against Equation Group, win and find out or bid pump price up, piss them off, everyone wins").

3. The tools, alongside information on clandestine NSA operations, were leaked in five waves between Aug. 13, 2016 and Apr. 14, 2017. For an in-depth account of the affair, see BUCHANAN, THE HACKER AND THE STATE: CYBER ATTACKS AND THE NEW NORMAL OF GEOPOLITICS 242-67 (Harvard Univ. Press 1st ed., 2020).

worldwide.[4] EternalBlue, an exceptionally powerful stolen intrusion tool which targets Windows computers, was the weapon behind the two most devastating cyberattacks in history—"WannaCry" and "NotPetya," which infected hundreds of thousands of computers in over 150 countries, causing billions of dollars in damage.[5]

The chain of events that led to the NSA losing control of EternalBlue was set in motion when the agency, having learned of the vulnerability in Windows systems, did not report it to Microsoft. The company could have created a patch and eventually did, after the leak.[6] The failure to notify Microsoft was not, however, a case of agency negligence, but rather a conscious decision by the U.S. intelligence community to stockpile and exploit software flaws for geopolitical and national security purposes.[7] This strategy, known as "vulnerabilities retention," is not strictly an American enterprise: governments all over the world spend billions of dollars to discover, develop, purchase, and, ultimately weaponize software flaws.[8] They do so as part of a growing trend of increased governmental presence in cyberspace, which has emerged as an all-important arena for politics, geopolitics

4. *See*, *e.g.*, Nicole Perlroth & Scott Shane, I*n Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc*, N.Y. TIMES (May 25, 2019), https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html [https://perma.cc/M5R7-KT9Z] (describing cyberattacks in the U.S. that have allegedly been enabled by exploits stolen from the NSA).

5. The WannaCry ransomware attack, believed to be by North Korea, broke on May 12, 2017, roughly a month after EternalBlue was leaked. Within four days, the malware was able to infect and encrypt the content of between 200,000–400,000 computers in dozens of countries. *See* DAVID E. SANGER, THE PERFECT WEAPON, 287–92 (2018). NotPetya was a Russian wiper-malware attack that initially targeted computers in Ukraine but soon spread globally, mostly to corporate networks. The malware wreaked havoc on countless businesses, medical facilities, governments, and homes. *See* Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018 5:00 AM), https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/ [https://perma.cc/W7M5-PYLG]. As of May 2019, there are believed to be over one million unpatched machines that can still be targeted by EternalBlue. *See Eternalblue: The NSA-developed Exploit That Just Won't Die*, SENTINELONE BLOG (May 27, 2019). https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/ [https://perma.cc/TBY4-5WLP].

6. The NSA never confirmed that it developed EternalBlue, but its origin has been confirmed by multiple sources, including Microsoft itself. *See* Brad Smith, *The Need for Urgent Collective Action to Keep People Safe Online: Lessons From Last Week's Cyberattack*, MICROSOFT ON THE ISSUES (May 14. 2017), https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#0Sdw18LTOG5EqR07.99 [https://perma.cc/22TA-LARC].

7. The process through which governments decide whether to disclose a vulnerability to the software vendor or exploiting it is known as "vulnerabilities equities process." *See infra*, Part V.B.

8. By their nature, intelligence expenditures are secret, so it is hard to ascertain the amounts devoted to specific line items. In 2013, the disclosures of Edward Snowden provided a rare glimpse at the U.S. secret "black budget," showing that in fiscal year 2013, the NSA funding for covert cyber operations was approximately 4.3 billion dollars. *See* Barton Gellman & Greg Miller, *'Black Budget' Summary Details U.S. Spy Network's Successes, Failures and Objectives*, WASH. POST (Aug. 29, 2013), https://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html [https://perma.cc/Y33P-FMG5].

and national security.[9]

There are two different angles to approaching the Shadow Brokers affair, and each epitomizes a strand in the literature on the role of the state in cyberspace. First, the affair can be viewed as a demonstration of the dangers of *government unaccountability* in cyberspace. Decisions to exploit, rather than report, software flaws are made in secret with minimal, if any oversight.[10] Leaks and other unintended consequences from storing vulnerabilities have direct and widespread effects on the population, which sets them apart from run-of-the-mill intelligence gathering. However, this practice is not subject to public rulemaking or review in any country. Put differently, checking mechanisms that liberal democracies typically put in place to ensure the accountability of the political executive do not cover this practice. This angle of the story resonates then with scholars who view cyberspace as a place that provides governments new pathways for control and coercion and worry over the inability of the legal system to respond timely.[11] They see governments resorting to surveillance, censorship, forced data "localization," and hacking, and fear that cyberspace is turning into a platform for executive aggrandizement.

Second, the fact that a group of unknown hackers was able to steal and render useless some of the NSA's most sophisticated and powerful cyberweapons may suggest that state power is in decline in the cyber sphere. It is inconceivable to imagine a fleet of F-35s stolen by criminals, but that is the equivalent of what happened to the NSA. This angle resonates with scholars who view the growing influence of various non-state actors in the cyber sphere, from criminals to multinational tech firms, as a sign that the role and, indeed, the power of national governments in cyberspace is diminishing.[12]

---

9. By "governmental presence in cyberspace," I mean both 'adversarial' government action such as hacking and spying, and governmental regulation of the internet and technology. *See*, *e.g.*, Jack Goldsmith & Andrew Woods, *Internet Speech Will Never Go Back to Normal*, THE ATLANTIC (Apr. 25, 2020), https://www.theatlantic.com/ideas/archive/2020/04/what-covid-revealed-about-internet/610549/ [https://perma.cc/PX37-587F] (providing examples and reasons for the trend "toward the growing involvement of government" in internet regulation).

10. *See infra* notes 273-79 and accompanying text.

11. This strand of scholarship largely originates from Jack Goldsmith & Tim Wu's WHO CONTROLS THE INTERNET (2006), which insisted that governments have many ways to exercise sovereign powers in cyberspace. While Goldsmith and Wu's work was mainly diagnostic and predictive, subsequent accounts have analyzed the normative implications of growing governmental use of, *e.g.*, surveillance technologies (BRUCE SCHNEIER, DATA & GOLIATH (2015)), big-data analytics (MICHAEL CHERTOFF, EXPLODING DATA (2018)), and inter-state hacking (ADAM SEGAL, HACKED WORLD ORDER, 31 (2d ed., 2017)).

12. This strand of scholarship mainly originates with the first generation of cyber theorists who, in the early days of the internet, envisioned cyberspace as a government-free zone. *See* David R. Johnson & David Post, *Law and Borders–The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367-68 (1996); John Perry Barlow, A Declaration of the Independence of Cyberspace (Feb. 8, 1996), https://www.eff.org/cyberspace-independence [https://perma.cc/TVK4-Z37K]. While this libertarian view of cyberspace never materialized, scholars have argued that, in cyberspace, governance-like functions assumed by non-state actors, especially multinational tech companies, carve out powers

We are left with a puzzle: the literature tells us, and the Shadow Brokers affair demonstrated, that governments are exceptionally powerful in cyberspace, and yet their sovereignty is being challenged more than ever by multiple actors. While these narratives are hard to reconcile, understanding the state of play is vital to ensure that legal and political responses to the government's increasing appetite to operate in and regulate cyberspace are appropriate. A lot is at stake: if the first part of the story captures the problem accurately, it means that public law and institutions should respond with rigor, keeping every attempted exercise of governmental power in cyberspace under scrutiny. If, however, the government is weak and constrained, and the real threats to digital liberty and rights come from other actors such as adversarial governments, criminals, and the tech giants, then clearly *more constraints* on the government from courts and the legislature would do no good. In this case, affording the government more flexibility and deference in "governing" cyberspace might be a wiser strategy.

In this Article, I challenge both narratives, by framing the debate somewhat differently. Instead of depicting government in cyberspace as either powerful or weak, I argue that its freedom of action is shaped by a web of interactions with exogenous forces and actors that exert their own force in the digital sphere. Examining these interactions reveals a new ecosystem of cyber checks and balances that has begun to take shape, in which independent forces defend their distinct interests and "ambition counteracts ambition".[13] Assessing this ecosystem requires a nuanced analysis, for the reason that its components do not only operate as "checks," nor do they target some passive, helpless entity. The Executive is an active participant in shaping and influencing this ecosystem and can change, overcome, and even exploit its constituent parts for its own needs. I examine the interactive moves and countermoves in Parts I-IV.

Part I focuses on the private sector. Private actors occupy a dominant position in the cyber domain, from which they can and do challenge governments. Their prominence stems from assuming roles in several important governance spheres, speech regulation, surveillance, collective cybersecurity, and international norm-making. From this position, private entities are perfectly situated to monitor and constrain numerous types of governmental activities in cyberspace. But the rise of private power, even

---

traditionally the province of nation-states. *See*, *e.g.*, Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 239 (2018) (arguing that the global nature of cyberspace "puts the multinational companies that manage our data in the position of mediating competing governmental demands and approaches, and ultimately determining the rules"); Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 187 (2018) ("internet companies challenge the state's monopoly over security, the very locus of traditional conceptions of sovereignty"); Kristen Eichensehr, *Digital Switzerlands*, 167 U. PENN. L. REV. 665 (2019) [hereinafter, Eichensehr, *Digital Switzerlands*] (examining the (self) portrayal of the world's largest internet companies as "Digital Switzerlands"); Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 199 (2017) (describing the major internet companies as "emergent transnational sovereigns").

13. *Cf.* THE FEDERALIST NO. 51 (James Madison) 321–22 (Clinton Rossiter ed., 1961) ("Ambition must be made to counteract ambition").

at the expense of governmental power, does not always translate into an effective check on the government. Sometimes, companies' interests are best served by cooperating with the government, and in these cases the leading role of the private sector can ultimately enhance rather than constrain government power.

Part II analyzes the checking role of the "architecture" of cyberspace. The idea that architecture is a force equivalent to law in its ability to constrain behavior is attributed to Professor Lawrence Lessig.[14] Lessig defines architecture as "the world as I find it," referring to the features of the material and virtual worlds that permit some actions and deny others.[15] In cyberspace, the ways software is designed, data is moved and stored, and infrastructure is owned and operated, create regulatory effects on what all users—including governments—can do. For example, encryption technology limits governmental access to data as it moves across cables and routers or is stored on the cloud. Like a statute that forbids trespass, the technology bans unauthorized users from accessing private on-line content. As will be shown, however, architectural constraints on government power can cut both ways, as governments are sometimes able to overcome technological barriers and even exploit them for their own needs.

International law is considered in Part III. International law is a normative constraint that prohibits exercises of state power in defiance of certain norms agreed upon by the international community. Cyberspace is a "space" that transcends national boundaries and shared by users from all countries. As such, state cyber activity is bounded by the rules of international law. Notably, however, international cyberlaw is still in its infancy and leaves many instances of state cyber activity unregulated or subject to normative ambiguities. As a result, paradoxically, the lack of regulation sometimes enhances rather than constrains state power.

Part IV focuses on international politics, a constraint that brings to bear power relationships on a global level. Suppose that State A fears that a certain course of action will elicit a response by State B that would harm State A's interests. If it decides to change course, then we can say that State A was constrained by international politics. In cyberspace, international politics generate significant new constraints; they are, however, imposed unevenly between democratic and non-democratic nations, to the detriment of democracies.[16] As will be shown, the United States is particularly prejudiced by this constraint.

---

14. In his famous accounts, Lessig described four "regulators," or, as he put it, four "modalities of constraint": law, social norms, market forces, and architecture. He initially introduced the idea as a general theory of regulation. *See* Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661 (1998) [hereinafter Lessig, *The New Chicago School*]. Subsequently, he applied and adapted the theory to cyberspace. *See* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999); LAWRENCE LESSIG, CODE: VERSION 2.0 (2006) [hereinafter LESSIG, CODE V. 2.0].

15. Lessig, *The New Chicago School*, *supra* note 14, at 663.

16. *See generally* Jack Goldsmith & Stuart Russel, *Strengths Become Vulnerabilities*, HOOVER INST. 4-15 (June 5, 2018).

Parts I–IV are mainly descriptive. Their goal is to explain how the different forces and actors of the digital ecosystem form a comparable of a checks and balances system. Part V turns to normative analysis. It concludes that given the opacity and unpredictability of the components of the ecosystem, it cannot be trusted to optimally check and balance governmental coercion in the digital sphere. But understanding how it operates yields valuable insights for our traditional constitutional checks and balances system. As will be demonstrated, it permits lawmakers, judges, and gatekeepers within the executive branch to better calibrate checking and balancing.

The theory advanced in this Article builds on the foundations of previous scholarship that studied the "diverse external ecosystem of actors who influence how the separation of powers plays out."[17] In cyber, scholars contributing to this theme in the literature have mainly focused on the checking role of the world's leading technology companies, overlooking the larger ecosystem in which these companies operate.[18] Aiming to fill this gap, this Article integrates several fields of scholarship, including international law, international relations, cybersecurity policy, and law and technology, which are analyzed from a public law perspective. The main contribution of this Article is constructing a complete picture of the exogenous forces and actors that constrain and empower the government in the digital sphere, thereby affording a better understating of how the cyber separation of powers works in practice. As more aspects of human activity go online, understanding how the government wields power, what forces shape its policies and actions, and how democratic accountability can be pursued more effectively, are matters of great importance to personal security, privacy, and liberty.

---

17. Aziz Z. Huq & Jon D. Michaels, *The Cycles of Separation-of-Powers Jurisprudence*, 126 YALE L.J. 346, 403 (2016). *See also* Ashley Deeks, *Secrecy Surrogates*, 106 VA L. REV. __ (forthcoming, 2021) (discussing the role of foreign allies, states, and localities, as well as the private sector in checking government abuses of secrecy privileges) [hereinafter Deeks, *Secrecy Surrogates*]; Ashley Deeks, *Checks and Balances from Abroad*, 83 U. CHI. L. REV. 65 (2016) (arguing that foreign actors "affect the quantum of power within the executive or the allocation of power among the three branches of the US government"); JACK GOLDSMITH, POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENCY AFTER 9/11(2012) (discussing the role of civil society organizations in checking the warmaking powers of the President); Daniel Abebe, *The Global Determinants of U.S. Foreign Affairs Law*, 49 STAN. J. INT'L L. 1 (2013) (arguing that international political variables should inform the level of deference accorded to the Executive by the legislature and the judiciary)

18. *See, e.g.*, Rozenshtein, *supra* note 12 (demonstrating how technology companies constrain the government's ability to conduct surveillance); Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467 (2017) [hereinafter, Eichensehr, *Public-Private Cybersecurity*] (describing how private actors wield power in cyberspace in ways that sometimes compete with and challenge government power); Deeks, *Secrecy Surrogates*, *supra* note 17 at *26–27 (showing how private monitoring of cyber incidents constrains intelligence agencies by challenging the government monopoly on intelligence); Samuel J. Rascoff, *Presidential Intelligence*, 129 HARV. L. REV. 633, 662–64 (2016) (discussing the function performed by American tech and communication firms in a "new intelligence oversight ecosystem").

## I. The Private Sector

> *"The flood of data about human and machine activity will put such extraordinary economic and political power in the hands of the private sector that it will transform the fundamental relationship, at least in the Western world, between government and the private sector."*[19]

"Governors,"[20] "competing power centers,"[21] "digital gatekeepers,"[22] and the "sovereigns of cyberspace"[23] are just a few of the terms used by scholars to describe the role of private technology companies in the digital ecosystem. The companies, for their part, seem to embrace these titles.[24] But while most of the scholarly focus has gone to the massive amounts of data that companies accumulate and their content moderation practices—and therefore to the impact of private ordering on free speech and privacy—we have somehow missed the bigger picture.[25] The technological revolution did not only provide online intermediaries with access to troves of personal data and (some) control over free speech, it has also reallocated significant political power from the state to the private sector on a massive scale. The evolution of the internet and of data-driven technologies has been a driver for encroachment of private companies into numerous spheres of governance. Today, companies are involved in an array of traditionally governmental functions, including international lawmaking, collective defense, law enforcement, electronic surveillance, and even the use of offensive (cyber) force. And the more that government services are automated, the more the dependency of the government in privately owned and operated systems will grow.[26]

---

19. Glenn S. Gerstell, *I Work for N.S.A. We Cannot Afford to Lose the Digital Revolution*, N.Y. TIMES (Sept. 10, 2019), https://www.nytimes.com/2019/09/10/opinion/nsa-privacy.html [https://perma.cc/WM3Z-KWVB]. Gerstell is the General Counsel of the NSA.

20. Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598 (2018).

21. Eichensehr, *Digital Switzerlands*, *supra* note 12.

22. Thomas E. Kadri, *Digital Gatekeepers* (forthcoming, 99 TEX. L. REV. 2021).

23. Jonathan Peters, *The "Sovereigns of Cyberspace" and State Action: The First Amendment's Application (or Lack Thereof) to Third-Party Platforms*, 32 BERKELEY TECH. L.J. 989 (2017).

24. Facebook CEO Mark Zuckerberg was quoted saying "in a lot of ways Facebook is more like a government than a traditional company." *See* DAVID KIRKPATRICK, THE FACEBOOK EFFECT: THE INSIDE STORY OF THE COMPANY THAT IS CONNECTING THE WORLD 254 (2011).

25. *See, e.g.*, Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149 (2018); Klonick, *supra* note 20; Hannah Bloch-Wehba, *Global Platform Governance: Private Power in the Shadow of the State*, 72 SMU L. REV. 27 (2019); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002). *But see* Eichensehr, *Digital Switzerlands*, *supra* note 12, at 702–12 (conceptualizing the cyberspace ecosystem as a triangle, "composed of three separate power centers: governments, technology companies, and users").

26. For early scholarship on the risks of automated decision-making in government, *see, e.g.*, Rory Van Loo, *Rise of the Digital Regulator*, 66 DUKE L.J. 1267 (2017); Ryan Calo & Danielle K. Citron, *The Automated Administrative State: A Crisis of Legitimacy*, 70 EMORY L.J. 797 (2021).

That the government is increasingly relying on private actors to perform key governance functions does not necessarily make it weak, or even weaker. But it does mean that private entities who in the past were clearly subordinate to governments and subject to their regulation are now more able to resist and impose costs on governments that advance policies harming their interests (and, by extension, their "users'" interests). This Part describes the variety of ways through which private actors can (and do) check governments. As will be shown, private checking has become common and prevalent. But lest we rush to celebrate the private sector's newfound role as the guardian of our constitutional entitlements, this Part concludes with a warning: the same conditions that enable private actors to engage in checking and balancing also permit collaboration and collusion with state authorities, which might turn out as a force multiplier for the government rather than a constraint. Companies, as for-profit corporations, ultimately act in ways that maximize their interests, and so understanding their varying incentives is crucial for assessing their role.

### A. Digital Private Ordering as a Constraint

Historically, the first and most important single decision that handed power from the government to private entities was the decision of the Clinton administration in 1994 to withdraw from internet management and let the private sector take over.[27] During the mid-1990s and early 2000s, internet governance has taken its new shape as a decentralized system dominated by non-governmental organizations like the Internet Engineering Task Force (IETF), the Internet Corporation for Assigned Names and Numbers (ICANN), and local internet providers and registrars. Even though the U.S. government kept its involvement in the internet as a regulator, the privatization of the entire enterprise has limited the access to and control of the state of information and catalyzed the birth of the digital economy.[28] Most of the focus of the U.S. government at the time was to support internet self-governance to promote liberty and innovation. As the new markets emerged and more areas of human activity went online, private actors began to perform more functions that are quintessentially forms of governance of human affairs and policymaking. Many governments have hoped that with the right use of sticks and carrots, they will be able to influence (if not dictate) how companies "govern". But, over time, the relationship between governments and companies evolved in some unpredictable ways: while governments frequently pressure companies to meet their local demands, companies have figured out that they have ways to push back, and that it is sometimes even in their interest to do so.

---

27. *See* Peter H. Lewis, *U.S. Begins Privatizing Internet's Operations*, N.Y. TIMES (Oct. 24, 1994). For an overview of the administration's policy on the internet in the late 1990s. *see* Ira C. Magaziner, *Creating a Framework for Global Electronic Commerce*, The Progress & and Freedom Foundation (Jul. 1999), http://www.pff.org/issues-pubs/futureinsights/fi6.1globaleconomiccommerce.html [https://perma.cc/TW47-Y2TH].

28. *See generally* Yochai Benkler, *How (if at all) to Regulate the Internet: Net Regulation: Taking Stock and Looking Forward*, 71 U. COLO. L. REV. 1203 (2000).

This is happening essentially in every policy domain in which private actors perform some governance function, including online speech regulation, surveillance, cybersecurity, and international policy advocacy.

Consider first the role of the major internet platforms in *speech regulation*. As billions of people all over the world create, consume, and share content online, their freedom of expression is governed by rules set and enforced by the platforms.[29] The rise of private governance of free expression created what Jack Balkin called a triangle of forces consisting of internet companies, national governments, and internet users.[30] While Balkin theorized the interaction between governments and internet companies as "relationships of cooperation, cooptation, and coercion,"[31] in which companies regulate speech and governments (mainly) regulate companies, he overlooked the fact that private speech regulation adds an important layer of private *oversight* on governmental efforts to censor or control online speech. Governments have no direct control over what happens on the platforms; when they seek to block certain speakers or remove content (this may be for legitimate reasons like blocking illicit materials or protecting IP rights but also for illegitimate reasons like deleting information critical of the government), they must go through the platforms. The platforms, on their part, can (and have) pushed back in a variety of ways, making governments' efforts at censorship harder, more costly, and sometimes impossible. The techniques for resisting governmental takedown requests range from insisting that proper procedures and all applicable law would be followed, to bringing legal challenges against the government in courts, publishing transparency reports about the volume and nature of requests, refusing removal requests, and exiting the market in extreme cases.[32] While flatly rejecting governmental removal orders is not very common and may provoke regulatory measures and sanctions against the companies, in recent years major internet platforms like Facebook, Google, and Twitter have clashed with the authorities in Canada,[33] Turkey,[34]

29. For an overview of content moderation practices, *see, e.g.*, TARLETON GILLESPIE, CUSTODIANS OF THE INTERNET 5–6 (2018); Klonick, *supra* note 20; Kyle Langvardt, *Regulating Online Content Moderation*, 106 GEO. L.J. 1353 (2018).

30. Balkin, *supra* note 25.

31. *Id.*, at 1188.

32. *See*, *e.g.*, Association for Progressive Communications, Content Regulation in the Digital Age: Submission to the U.N. Special Rapporteur on the Right to Freedom of Opinion and Expression 8 (Mar. 2018) (providing recommendations for responding to governmental takedown requests); Spandana Singh & Kevin Bankston, *The Transparency Reporting Toolkit: Content Takedown Reporting*, NEW AMER. (Oct. 15, 2018), https://www.newamerica.org/oti/reports/transparency-reporting-toolkit-content-takedown-reporting/ [https://perma.cc/AV79-DPCX] (offering internet companies general best practices for content takedown).

33. Google Inc. v. Equustek Solutions Inc., 2017 SCC 34 (Can.).

34. David Gauthier-Villars, *Twitter, Facebook Fined by Turkey for Breaching Law Aimed at Curbing Dissent*, WALL ST. J. (Nov. 4, 2020, 11:06 AM), https://www.wsj.com/articles/twitter-facebook-fined-by-turkey-for-breaching-law-aimed-at-curbing-dissent-11604501440 [https://perma.cc/T8BB-RQVQ].

India,[35] Egypt,[36] Singapore,[37] the EU,[38] and other places over content removal. In a recent example, in response to proposed anti-doxing legislation[39] which can adversely affect free speech in Hong-Kong, Facebook, Twitter, and Google have threatened to stop offering their services in the city.[40] Given the market power of the companies and the significance of the platforms, such strategies exert pressure on governments and help check governmental attempts to restrict online speech.

Similar dynamics are at play when governments seek to obtain personal data held by the private sector for *surveillance*. The endless trove of data recorded by internet companies is of great interest to governments, as it may help solve or prevent crimes or contain valuable information for intelligence agencies. Since the beginning of the internet, governments have sought, in many ways—cooperative, coercive, and covert—to gain access to the private infrastructure on which user-data traveled and are stored. Secret partnerships with telecom providers,[41] programs like PRISM (United States), and TEMPORA (U.K.) that legally compelled companies to produce data,[42] and covert efforts to tap fiber optic connections of major companies without their knowledge,[43] have all successfully served the same goal: harnessing the surveillance capabilities of the private sector to extend the reach of government surveillance, both *technically* by acquiring access to data otherwise unavailable to government agencies and *legally* by

35. Jeff Horwitz, *Facebook Blocks, Then Restores, Content Calling on Indian Prime Minister Modi to Resign*, WALL ST. J. (Apr. 8, 2021, 9:41 PM), https://www.wsj.com/articles/facebook-blocks-then-restores-content-calling-on-indian-prime-minister-modi-to-resign-11619652354 [perma.cc/LM8S-U9HM].

36. Erick Schonfeld, *Twitter Is Blocked in Egypt Amidst Rising Protests*, TECHCRUNCH (Jan. 25, 2011, 10:41 AM), https://techcrunch.com/2011/01/25/twitter-blocked-egypt/ [perma.cc/7W7J-9UA3].

37. Fathin Ungku, *Singapore Lawmaker Blasts Facebook Over Refusal to Take Down 'False' Post*, REUTERS (Nov. 20, 2018, 2:31 AM), https://www.reuters.com/article/us-singapore-politics-facebook-idUSKCN1NP0KZ [https://perma.cc/3EZS-JVDE].

38. Conseil d'État [CE] (Council of State), (Sept. 24, 2019) C-507/17.

39. The term "doxing" refers to the act of revealing identifying information about someone online without one's consent.

40. Newley Purnell, *Facebook, Twitter, Google Threaten to Quit Hong Kong Over Proposed Data Laws*, WALL ST. J. (July 5, 2021), https://www.wsj.com/articles/facebook-twitter-google-warn-planned-hong-kong-tech-law-could-drive-them-out-11625483036 [https://perma.cc/WV9K-PEL8].

41. *See* Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J. L. & TECH. 1, 55 (2003); *see also* Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CAL. L. REV. 901, 910–17 (2008) (providing examples of secret collaborations between the U.S. government and American telecom companies).

42. For an overview of PRISM, see Privacy & Civil Liberties Oversight Bd., Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (Jul. 2, 2014). For an overview of TEMPORA, *see* Big Brother Watch v. The U.K., App nos. 58170/13, 62322/14 and 24960/15 (2018).

43. Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST (Oct. 30, 2013), https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html [https://perma.cc/2994-A2EN].

skirting legal prohibitions that do not apply to private surveillance.[44]

But as scholars have shown, under the current system of production of user data to public authorities, the companies function as "surveillance intermediaries,"[45] or the "middle-man,"[46] or the people's "corporate avatars"[47]—perfectly situated to monitor the government and limit unlawful or unwarranted governmental access to personal data. As Alan Rozenshtein's 2018 article, *Surveillance Intermediaries*, has shown, internet companies use various techniques to check government surveillance.[48] For example, they resort to legalism. Namely, instead of handing data to public authorities secretly and informally upon request—a common practice for telecom companies in the pre-digital era—internet companies insist on formal requests that are subject to legal procedures and oversight. In general, the more private and invasive the information required by public authorities, the higher the legal threshold for compelling its production. And thus, as he explains, "forcing the government to use formal legal process adds friction to what might otherwise be a smooth relationship of informal collaboration."[49] Moreover, when companies believe that orders to hand over personal data are too broad or otherwise legally invalid, they challenge them in court.[50] Companies rarely prevail in litigation and researchers have questioned the effectiveness of their arguments in court as well as their commitment to users,[51] but litigation, especially in high profile cases, provokes public debate on government access to personal data and energizes efforts to bring surveillance under tighter legal control.[52]

Another area in which the private sector makes governmental coercion harder is *cybersecurity*. Companies play several roles in cybersecurity: some are principal targets for cyberattacks and data theft,[53] others are points of entry for intrusions to public networks and systems,[54] and still

---

44. *See* Niva Elkin-Koren & Eldar Haber, *Governance by Proxy: Cyber Challenges to Civil Liberties*, 82, 107 BROOK. L. REV. (2016) ("Informal [public-private partnerships] enable governments to bypass constitutional constraints because private bodies are not subject to constitutional limits on search or censorship and are under no duty to respect free speech or other fundamental rights"); Daphne Keller, *Who Do You Sue? State and Platform Hybrid Power over Online Speech*, Aegis Series Paper No. 1902, HOOVER INST. 2 (2019).

45. Rozenshtein, *supra* note 12.

46. Jack M. Balkin, *The First Amendment in the Second Gilded Age*, 66 BUFF. L. REV. 979, 993 (2018).

47. Avidan Y. Cover, *Corporate Avatars and the Erosion of the Populist Fourth Amendment*, 100 IOWA L. REV. 1441 (2015).

48. *See* Rozenshtein, *supra* note 12, at 122–49.

49. *Id.* at 123.

50. *See, e.g.*, Gonzales v. Google, Inc., 234 F.R.D. 674 (N.D. Cal. 2006).

51. *See* Cover, *supra* note 47, at 1463–67; Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1940–41 (2013).

52. *See* Rozenshtein, *supra* note 12, at 148–49.

53. *See* discussion *supra* note 5.

54. *See, e.g.*, FireEye, *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor* (Dec. 13, 2020), https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html [https://perma.cc/UE9R-RTCG].

others are partners of the government in the provision of collective cyber defense.[55] Private governance in cybersecurity is in large part a consequence of these multiple roles. A convergence of interests and complementarity of capabilities have led private and public actors to work side by side, often in a sort of informal partnership, in the battle over cyberspace. As noted by the U.S. Cyber Commission, the private sector carries much of the burden in this partnership:

> [C]yber defense, while a shared responsibility, will depend significantly on the underlying efforts of the owners and operators of private networks and infrastructure. National defense therefore takes a very different shape in cyberspace, where the government mainly plays a supporting and enabling role in security and defense and is not the primary actor.[56]

However, the interface between the private sector and the government in the realm of cybersecurity creates friction as well. It enables the private sector to watch and monitor state activity that is otherwise shrouded in secrecy. When that activity clashes with the interests of the private sector, companies have ways to expose, impose costs on, and even frustrate it. Consider, for example, the increased involvement of companies in intelligence and counterintelligence. Many technology companies now have inhouse specialized threat intelligence teams—analysts whose role is to gather and analyze data on security threats.[57] A common practice in the cybersecurity industry is to perform public attributions of cyberattacks: to expose and shame states involved in malicious cyber incidents.[58] Similarly, popular internet platforms like Google and Facebook engage in attribution to protect their users. These companies regularly send warnings to users whose accounts have been targeted by state-sponsored hackers.[59]

The evolution of intelligence expertise within the private sector allows companies to check governments in at least three ways. First, it enhances

---

55. *See generally* Eichensehr, *Public-Private Cybersecurity*, *supra* note 18; Madeline Carr, *Public-Private Partnerships in National Cyber-security Strategies*, 92 INT'L AFF. 43 (2018).

56. *See* U.S. CYBERSPACE SOLARIUM COMM'N, OFFICIAL REPORT, 96 (2020) [hereinafter SOLARIUM COMM'N REP.].

57. Cybersecurity vendors like Mandiant (FireEye), Crowdstrike, and McAfee are widely known for their high-level intelligence gathering capabilities, but threat intelligence is also practiced by large software and internet companies, such as Microsoft and Facebook.

58. Scholars have noted that this practice is motivated mainly by business considerations. *See, e.g.*, ASHA ROMANOSKY & BENJAMIN BOUDREAUX, RAND CORP., PRIVATE SECTOR ATTRIBUTION OF CYBER INCIDENTS: BENEFITS AND RISKS TO THE U.S. GOVERNMENT 6–12 (2019) (arguing that "firms publicly attribute in part to demonstrate the competence of the company, to raise its profile, and develop additional business opportunities"); Eichensehr, *Public-Private Cybersecurity*, *supra* note 18, at 489 (arguing that cybersecurity firms make public attributions of attacks "for marketing purposes and to generate business").

59. *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/7VVK-M3GY].

accountability. Victim states are often reluctant to publicly attribute attacks due to various geopolitical calculations (e.g., calling out another state for a type of activity that the victim engages with regularly might be self-implicating).[60] Having companies monitoring state-to-state attacks, which are becoming major source of instability in the world, means that overall, more attacks will be publicly attributed.[61] Aware of their enhanced visibility, the attacking governments likely would be more restrained, before engaging in offensive cyber operations. Second, attributions by private companies increase transparency. These attributions tend to be more detailed than when governments make them.[62] Detailed reports provide outside observers with the access to granular information about cyber threats and improve transparency in a domain otherwise subject to extreme secrecy.[63] And third, private intelligence expertise puts firms in a position to challenge and vet attributions made by governments and the validity of the intelligence underpinning them.[64] The lack of universally accepted evidentiary standards for attributions increases the risk that governments would make false or erroneous accusations or rely on unsubstantiated inferences from available data. Private-public information sharing, which, as noted, both sides have reasons to maintain, mitigates that risk by allowing companies the opportunity to evaluate findings shared by the government. This is an exceptionally valuable check in a field known for its lack of strong oversight.

Finally, the private sector constrains government by stepping into the field of *international law-making*. In recent years, technology companies have been deeply involved in the global effort to form international rules of behavior that would restrict the growing resort to offensive cyber operations by states and state-backed actors.[65] Microsoft, whose products have been exploited for some of the most destructive state-sponsored cyberattacks in history,[66] has been at the forefront of many of these efforts. The company published two white papers, one putting forward norms for limiting conflict in cyberspace and the other calling for the creation of a "digital Geneva Convention" to protect civilians and civilian infrastructure.[67]

60. *See* Kristen E. Eichensehr, *The Law & Politics of Cyberattack Attribution*, 67 UCLA L. REV. 520, n.126 (2020) [hereinafter, Eichensehr, *Cyberattack Attribution*].

61. *Id.*, at 547–50.

62. *See* Romanosky & Boudreaux, *supra* note 58, at 10 (describing the common structure of threat reports by cybersecurity firms).

63. *See* Eichensehr, *Cyberattack Attribution*, *supra* note 60, at 548.

64. Deeks, *Secrecy Surrogates*, *supra* note 17, at *29–32.

65. Participation of private actors in international lawmaking is not a new phenomenon: NGOs, research institutions, and civil society organizations have been involved in and even led lawmaking initiatives in areas spanning from climate change to counterterrorism. What is unique about cyber is that many of the initiatives are led by for-profit corporations, specifically the world's largest tech companies, which seem poised to regulate governments—normally their own regulators.

66. Examples include the WannaCry ransomware attack (2017) and NotPetya wiper-malware attack (2017). *See* discussion *supra* note 5.

67. MICROSOFT, INTERNATIONAL CYBERSECURITY NORMS: REDUCING CONFLICT IN AN INTERNET-DEPENDENT WORLD (2015); MICROSOFT, A DIGITAL GENEVA CONVENTION TO PROTECT CYBERSPACE (2017).

Moreover, Microsoft advocated an active role for the private sector in observing these norms. Brad Smith, the company's President, announced that "the tech sector plays a unique role as the internet's first responders, and we therefore should commit ourselves to collective action that will make the internet a safer place, affirming a role as a neutral Digital Switzerland that assists customers everywhere and retains the world's trust."[68]

Other initiatives soon followed.[69] Over 100 companies, including Facebook, Microsoft, and LinkedIn, signed the Cybersecurity Tech Accord (CTA), an initiative calling on the private sector to safeguard cybersecurity and oppose attacks on civilians and businesses worldwide, regardless of their origin or goal.[70] Leading European companies, including Siemens, instituted the Charter of Trust, adopting measures to strengthen security, protect user data, and prevent damage to individuals and businesses.[71] In other examples, tech companies partnered with or financially supported international, academic, and civil society proposals: Microsoft is the co-founder of the Global Commission on the Stability of Cyberspace, a group of experts proposing cybersecurity norms for state and non-state actors.[72] The CTA signatories participate and support the Geneva Dialogue on Responsible Behaviour in Cyberspace, a project tackling the proper allocation of roles of different stakeholders in promoting peace and security in cyberspace.[73] Bank of America, Cisco, and General Electric are among the companies supporting the Carnegie Endowment's Norm Against Manipulating Financial Data, which seeks to "promote the resilience of financial services and institutions" against cyber-attacks.[74] Each proposal seeks to

68. Brad Smith, *The Need for a Digital Geneva Convention, Remarks at the RSA Conference*, MICROSOFT (Feb. 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/ [https://perma.cc/22AZ-H8M3]. Smith is the President and Vice Chair of Microsoft. In addition, Microsoft advocated the creation of an international body to handle attribution of cyber-attacks. *See* Herb Lin, *Microsoft Proposes an Independent Body for Making Attribution Judgments*, LAWFARE (June 24, 2016, 3:50 PM), https://www.lawfareblog.com/microsoft-proposes-independent-body-making-attribution-judgments [https://perma.cc/U83T-3NKU].

69. For an in-depth description of private-led global cyber policy initiatives, *see* Ido Kilovaty, *Privatized Cybersecurity Law*, 10 U.C. IRVINE L. REV. 1181 (2020).

70. *See* Cybersecurity Tech Accord, https://cybertechaccord.org/ [https://perma.cc/27LL-3FXG] (last visited Oct. 31, 2022).

71. SIEMENS, CHARTER OF TRUST ON CYBERSECURITY (Apr. 2019), https://assets.new.siemens.com/siemens/assets/public.1560760957.55badda4-4340-46d3-b359-f570e7d1f4c2.charter-of-trust-presentation-en.pdf [https://perma.cc/92DE-U353]. As of February 2020, the initiative expanded to 17 signatories, including companies from Asia and North America.

72. GLOBAL COMM'N ON THE STABILITY OF CYBERSPACE, ADVANCING CYBERSTABILITY: FINAL REPORT 18–25 (Nov. 2019), https://hcss.nl/wp-content/uploads/2019/11/GCSC-Final-Report-November-2019.pdf [https://perma.cc/7QP5-4EAZ].

73. *See* Geneva Dialogue on Responsible Behaviour in Cyberspace, *Fact Sheet: Geneva Dialogue on Responsible Behaviour in Cyberspace* (June 2018), https://www.diplomacy.edu/wp-content/uploads/2018/07/201806_Factsheet_GDRBC.pdf [https://perma.cc/W2TW-C8WT].

74. Tim Maurer et al., *Toward a Global Norm Against Manipulating the Integrity of Financial Data*, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE (2018), https://carnegieendowment.org/files/Cyber_Financial_Data_white_paper.pdf [https://perma.cc/LXP2-4ZG8].

advance norms of conduct that impose significant constraints on states carrying out offensive cyber activities.

Private actors, it should be remembered, lack formal international lawmaking status, and their initiatives are not binding on nation states. But the corporate push for a cyber environment governed by legal norms does put pressure on states and has the potential to exert strong normative influence. Each initiative broadens the conversation, emphasizes the need to restrain states' behavior, and stimulates more debate and action.[75] Widely publicized and accessible free on-line, private policy and lawmaking initiatives serve as the first and sometimes only points of reference, indirectly shaping the legal terrain for what will be considered acceptable state behavior. Moreover, the attention that some private initiatives attract from the media, the market, and leading experts, challenges states to respond and take part in the conversation, which in and of itself corners them to take a stand on the issues. This may prove to have legal significance as an articulation of *opinio juris* (a belief that a norm represents a legal obligation), a critical condition in the formation process of customary law. The Paris Call for Trust and Security in Cyberspace is a good example of how private leadership induces a state response.[76] Building on its previous work, Microsoft worked closely with the French government on the Call, a commitment containing nine core principles to secure cyberspace.[77] To date, the Call has been endorsed by 81 states and 706 companies.[78]

### B. Private-Public Collaborations and the Risk of Government Aggrandizement

The emergence of private participation in a range of traditional public domains creates plenty of opportunities for private corporations to check the government's cyber activities. But in the same fashion, the intersection of state and private power creates opportunities for private-public *collaboration*, whose impact on government power is empowerment rather than constraint. For example, scholars argued that on balance, "surveillance intermediaries" make it easier for the government to obtain personal data, even though they resist from time to time.[79] It is indeed burdensome to have to issue formal letters and battle in courts to gain access to user content, but in a world without surveillance intermediaries the government

75. *Cf.*, Yahli Shereshevsky, *Back in the Game: International Humanitarian Lawmaking by States*, 37 BERKLEY J. INT'L L. 1, 38–41 (2019) (discussing the importance of first initiatives in shaping the international legal landscape).

76. Emmanuel Macron, President of the French Republic, Paris Call for Trust and Security in Cyberspace (Nov 12, 2018).

77. Michel Rose, *Macron and tech giants launch 'Paris call' to fix internet ills*, REUTERS (Nov. 12, 2018), https://www.reuters.com/article/us-cyber-un-macron-idUSKCN1NH0FS [https://perma.cc/D8AE-HYR9].

78. *See* PARIS CALL FOR TRUST AND SECURITY IN CYBERSPACE, https://pariscall.international/en/ [https://perma.cc/R4YN-5TNV] (last visited Feb. 9, 2022).

79. Cover, *supra* note 47, at 1492; *see also* Note, *Cooperation or Resistance?, The Role of Tech Companies in Government Surveillance*, Developments in the Law, 131 HARV. L. REV. 1722, 1724 (2018).

would have never been allowed to access so much personal information of so many people, locals and foreigners.[80] As Bruce Schneier noted, corporate-government surveillance partnership "allows both the government and corporations to get away with things they couldn't otherwise."[81] In a similar vein, internet platforms frequently acquiesce government takedown requests. While many removals are required by local law and refusal can result in sanctions against the platform,[82] no less troubling are what the Electronic Frontier Foundation referred to as "shadow regulation"—invisible arrangements between platforms and governments.[83] In Israel, for example, the cyber unit of the State Attorney's Office maintains ties with Facebook and other platforms for deleting illicit content.[84] The unit operates in this capacity without clear legal basis and with no transparency, yet removal decisions are not subject to constitutional protections because they are formally made by the platforms, not the government.[85] The result of cooperation then is that the government is able to censor speech in ways that bypass critical democratic safeguards, when the only actor in its way are the companies. It is not unlikely to assume that companies might overcomply with takedown requests to avoid the threat of more regulation and sanctions. When this is the outcome, companies not only fail to check governments, but in practice enhance their power.

It is ultimately up for the companies to decide whether to assist or resist governments. As for-profit corporations, economic considerations are the main drivers in their decisionmaking, but these are shaped by a range of second-order factors like reputation, brand, expectations of their paying customers and non-paying users, organizational culture, business model, and other factors that vary across companies, time, and place. As scholars noted, for example, American internet and telecom companies assisted the government more after the 9/11 attacks and resisted more fol-

80. *See* Michael Hirsh & Nat'l. J., *Silicon Valley Doesn't Just Help the Surveillance State—It Built It*, THE ATLANTIC (June 10, 2013), https://www.theatlantic.com/national/archive/2013/06/silicon-valley-doesnt-just-help-the-surveillance-state-it-built-it/276700/ [https://perma.cc/T452-L7BW].

81. Bruce Schneier, *The Public-Private Surveillance Partnership*, SCHNEIER ON SECURITY (July 31, 2013), https://www.schneier.com/essays/archives/2013/07/the_public-private_s.html [https://perma.cc/QQ7M-7NYA].

82. *See* Facebook Transparency Ctr., Content Restrictions Based on Local Law—H2 2020 Report, https://transparency.fb.com/data/content-restrictions [https://perma.cc/6HL4-QVZK] (last visited: June 30, 2021).

83. *See* Jeremy Malcolm & Mitch Stoltz, *Shadow Regulation: the Back-Room Threat to Digital Rights*, ELECTRONIC FRONTIER FOUND., (Sept. 29, 2016), https://www.eff.org/deeplinks/2016/09/shadow-regulation-back-room-threat-digital-rights [https://perma.cc/G3ZP-5DCH].

84. *See* Association for Progressive Communications, *supra* note 32, at 10.

85. Recently, a petition challenging the legality of this practice were rejected at the Supreme Court. *See* HCJ 7846/19 Adalah Legal Center for Arab Minority Rights in Israel v. State Attorney's Office – Cyber Department (2021) (Isr.). For commentary, see Tomer Shadmy & Yuval Shany, *Protection Gaps in Public Law Governing Cyberspace: Israel's High Court's Decision on Government-Initiated Takedown Requests*, LAWFARE (Apr. 23, 2021, 10:55 AM), https://www.lawfareblog.com/protection-gaps-public-law-governing-cyberspace-israels-high-courts-decision-government-initiated [https://perma.cc/46NF-2RA3].

lowing the Snowden scandal.[86] In addition, companies are not monolithic entities, and may be affected by different stakeholders with diverging motives.[87] At times, their interests will align with the public interest, but this is not always the case. More research is required to fully unpack the incentive structures that shape company behavior in varying situations and places. But the available evidence is indicative that friction between the private sector and the government arises frequently across various policy domains. From a checks and balances perspective, this friction is likely to serve liberty and the public interest in the long run.

## II. The "Architecture" of Cyberspace

*"Architecture is a kind of law: It determines what people can and cannot do."*[88]

For the first generation of scholars studying the relationship between government power and the internet, the architecture of information communication technologies was perhaps the most compelling reason why cyberspace was going to be immune to government regulation. In 1996, David Johnson and David Post argued that the cross-border nature of virtual space renders any effort to enforce geographically-based laws in that space illegitimate and unfeasible.[89] They meant that a basic feature of how the internet was designed—its disregard of territorial boundaries—constrains governments seeking to assert their sovereignty. As later elaborated by Lessig and others, the code that determines how software works; the password that limits unauthorized access; the privately owned cables and exchange points through which data travel; and the locations and systems in which information is stored are illustrations of how architecture creates "regulatory" effects that determine what users, including government users, can and cannot do.[90]

This Part begins by demonstrating how these features of "architecture" place limits on governmental coercion in cyberspace. It then shows how governments have found ways to circumvent and even explore the con-

86. *See, e.g.*, Cohen, *supra* note 12, at 193; *see also* Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1127 n.401 (2016).

87. *See, e.g.*, Sheera Frenkel & Mike Isaac, *India and Israel Inflame Facebook's Fights With Its Own Employees*, N.Y. TIMES (June 4, 2021), https://www.nytimes.com/2021/06/03/technology/india-israel-facebook-employees.html [https://perma.cc/ZP44-PPJ3] (reporting internal divisions within Facebook over the company's handling of content moderation in India and Israel).

88. LESSIG, CODE V. 2.0, *supra* note 14, at 77.

89. Johnson & Post, *supra* note 12, at 1367–68.

90. *See generally* LESSIG, CODE V. 2.0, *supra* note 14, at 121–25 (describing how "the software and hardware that make cyberspace what it is constitute a set of constraints on how you can behave"); R. Polk Wagner, *On Software Regulation*, 78 S. CAL. L. REV. 457, 457 (2005) ("The most significant principle to emerge from the academic study of law on the Internet is the idea that software code—the applications, operating systems, and protocols that determine the way we experience the online world—is broadly substitutable for legal code—the regulatory infrastructure of society"); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 554 (1998) ("Technological capabilities and system design choices impose rules on participants").

straints imposed by the technology. This duality best captures the role of architecture in the cyber checks and balances ecosystem: at times, it is an effective check, while at others, it enhances the risks of governmental overreach.

### A. How Algorithms Constrain

Government cyber activity—whether for surveillance, law enforcement, or any other purpose—requires access to infrastructure and systems beyond government control. For example, if country A wants to obtain data that contain sensitive military or diplomatic materials of country B, it must first gain access to that data at some point en route or at the location where the data are stored. This can be done in one of two ways: the first, known as passive collection, is the practice of intercepting data from telecommunications cables and hubs through which data travel across the world.[91] The second, active collection, refers to the practice of hacking a computer to acquire illicit access, allowing the hacker to steal information from the targeted computer, as well as from other computers and servers on its network.[92] From country A's perspective, the problem is that the cables, hubs, networks and systems on which data travel and are stored were designed with the purpose of blocking such access. Wherever data is found online, there are technical, or architectural, limitations that inhibit the ability of unauthorized parties to obtain access. These limitations are crucial for the functionality of the internet as a medium for communication and commerce, and they protect socially desirable values like privacy, free speech, and free enterprise.[93] These limitations also burden government data collection.

Encryption, the mathematical process of transforming information into a form incomprehensible to anyone but the original owner and intended recipient, serves as a paradigm. Many online services and hardware manufacturers now encrypt information, both "in transit," when traveling between the sender and recipient, and "at rest," when stored on the cloud or on hard drives.[94] Some encryption platforms provide the decryption key— data necessary to recover the original information—only to the sender and recipient, known as end-to-end encryption, while others keep a copy of the key, so that the service provider has third-party access.[95] Encryption is always intended to deny unauthorized access and the manipulation of data. Similar to a law that prohibits access, encryption produces a constraint, by rendering the data worthless to anyone who does not have

91. *See* BUCHANAN, *supra* note 3, at 18. (2020).

92. *Id.*, at 242–67.

93. David Kaye, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, at 3 A/HRC/29/32 (May 22, 2015).

94. *See* Berkman Ctr. for Internet & Soc'y, *Don't Panic: Making Progress on the "Going Dark" Debate,* HARV. U. 3–4 (2016), https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [https://perma.cc/P6LU-AZ8A] [hereinafter, Berkman Ctr. Report].

95. For an overview of how cryptography secures data, see, e.g., KEITH M. MARTIN, EVERYDAY CRYPTOGRAPHY, 2–39 (2d Ed., 2017).

the decryption key.[96] To be sure, architecture does not have exactly the same effect as law. Unlike law, it does not seek to impose rules but rather to establish facts, technologically curtailing the capacity of the government to access unauthorized information.[97]

In the wake of the Snowden revelations, encryption has gained market recognition as a vital tool for protecting users from government surveillance.[98] In 2014, Apple and Google adopted an encryption-by-default policy in their mobile operating systems. Shortly thereafter, WhatsApp integrated end-to-end encryption in its product, with other instant messaging apps, such as Telegram, Signal, Cyphr, Apple's iMessage, and Facebook Messenger, following suit.[99] As the trend accelerated and the industry showed a greater appetite for privacy-focused products,[100] encryption grew into a problem for law enforcement and intelligence agencies around the world.[101] In what has been labeled as the "going dark" problem,[102] the FBI warned Congress that ubiquitous encryption "poses real barriers to law enforcement's ability to seek information in specific cases of possible national security threat."[103] A leaked NSA document from 2012 revealed that beating encryption was a top priority for the agency,[104] and as another document put it, the "price of admission for the [United States] to

96. For the view of encryption as a substitute for legal prohibitions on surveillance, see Ryan Calo, *Can Americans Resist Surveillance?* 83 U. CHI. L. REV. 23 (2016).

97. *Cf.*, Daryl J. Levinson, *Incapacitating the State*, 56 WM. & MARY L. REV. 181, 195–202 (2014) (referring to this approach as "incapacitation").

98. *See* Hannah Kuchler, *Tech Companies Step Up Encryption in Wake of Snowden,* FINANCIAL TIMES (Nov. 4, 2014).

99. This trend is important, but it should not be overstated. For many data-driven companies, adopting end-to-end encryption runs contrary to their business model, which relies heavily on targeted advertising and requires company access to user data. *See* Berkman Ctr. Report, *supra* note 94, at 9–10.

100. *See* Kuchler, *supra* note 98 (noting that "the technology heavyweights have been joined by a new cast of privacy-focused start-ups who are creating apps and hardware with better security. From the Wickr messaging app to the Blackphone by Silent Circle, venture capitalists are pouring money into companies catering for a privacy-focused audience").

101. *See* SOLARIUM COMMI'N REP., *supra* note 56, at 95 (noting that "end-to-end encryption is currently impeding the government's ability to obtain lawful access to electronic evidence in investigations ranging from cyber intrusions and attacks to crimes threatening serious harm"). To be sure, the beginning of the public debate over the propriety of giving law enforcement authorities exceptional access to encrypted information preceded the Snowden scandal–it broke out in the U.S. in the early 1990s. *See generally* A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995).

102. *See* Going Dark: Lawful Electronic Surveillance in the Face of New Technologies, Before the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary, United States House of Representatives, 112th Cong. (2011).

103. Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy: Hearing Before the S. Comm. on the Judiciary, 114th Cong. 1 (2015) (joint statement of James B. Comey, Dir., Fed. Bureau of Investigation, and Sally Quillian Yates, Deputy Att'y Gen., Dept. of Justice). For additional statements by security establishment officials, see Berkman Ctr. Report, *supra* note 94, at 6–7.

104. BUCHANAN, *supra* note 3, at 46.

maintain unrestricted access to and use of cyberspace."[105] The British Government Communications Headquarters (GCHQ) openly asked providers to change their software code to enable governments "exceptional access" into encrypted communications—as might be expected, their proposal met strong opposition in the tech industry.[106] Overall, the resources and effort devoted to the issue by law enforcement and intelligence agencies indicated that these communities see encryption as a meaningful architectural constraint on their power.

Belying the perception created by the "going dark" metaphor, law enforcement and intelligence agencies in the United States and the U.K. have responded to the challenge.[107] Though nearly all of the government activity to crack encryption is done in secret and it is likely that many of the tools and methods used are unknown, journalists and academics were able to obtain leaked, and declassified materials and forensic reports revealed some of the ways by which governments have broken or circumvented encryption.[108]

The Snowden files, the source of many of these revelations, provided a glimpse of the scope of the effort and the multiplicity of ways employed. While apparently no one method was able to decipher every bit of encrypted data, the cumulative effect has been transformational. To cite a few examples, this multi-pronged effort included the use of supercomputers to crack encryption keys with brute force, namely, beating cryptographic barriers with superior computational power and mathematical skills;[109] the development of a secret database of encryption keys for specific products, which, according to estimates, were obtained by hacking

105. *Id.*

106. *See* Dan Sabbagh, *MI5 Chief Asks Tech Firms for 'Exceptional Access' to Encrypted Messages*, GUARDIAN (Feb. 25, 2020, 12:35 PM), https://www.theguardian.com/uk-news/2020/feb/25/mi5-chief-asks-tech-firms-for-exceptional-access-to-encrypted-messages [https://perma.cc/F8VC-A3RB].

107. To begin with, encryption only impedes passive collection. Active measures that target data before encryption or after decryption bypass this problem, and for states that use active hacking, the concept of "going dark" to describe the challenges of ubiquitous encryption seems inaccurate.

108. *E.g.*, BUCHANAN, *supra* note 3, at 40–85; Alex Halderman & Nadia Heninger, *How is NSA Breaking so Much Crypto?*, FREEDOM TO TINKER – PRINCETON U. CTR. FOR INFO. TECH. POL'Y (Oct. 14, 2015), https://freedom-to-tinker.com/2015/10/14/how-is-nsa-breaking-so-much-crypto/ [https://perma.cc/KQG9-7JNM]; Spiegel staff, *Inside the NSA's War on Internet Security*, DER SPIEGEL (Dec. 28, 2014, 8:01 PM), https://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html [https://perma.cc/Z3NC-WQZA]; James Ball, Julian Borger and Glenn Greenwald, *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security*, THE GUARDIAN (Sept. 6, 2013, 11:24 AM), https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security [https://perma.cc/8RRZ-TTVE]; Nicole Perlroth, et. al, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES (Sept. 5, 2013), https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?hp&_r=0 [https://perma.cc/X7L3-6T7Y].

109. *See* BUCHANAN, *supra* note 3, at 47–51 (detailing the investments and effort made by the NSA to acquire cryptographic supremacy).

into the servers of key producers;[110] and the deployment of special spying units to monitor and covertly shape the standards set for security and encryption by cellphone and internet firms around the globe. This last step has helped anticipate what new methods of encryption these companies would adopt in the future and ensured that collection measures kept pace.[111] Other aggressive methods included secret corporate partnerships, through which agencies covertly inserted backdoors in encrypted products;[112] and acquisition of software security vulnerabilities from hackers and cybersecurity contractors, allowing the agencies to create backdoors without the software company's knowledge.[113] Thanks to these and other efforts, a huge amount of data encrypted by its user and believed to be secured became available to the intelligence community.

However important, encryption is but one of many architectural constraints. By resorting to similar methodologies—efforts that rely on the agencies' vast resources, legal authority, sophistication, and relationships—the intelligence and law enforcement communities have circumvented other constraints. Cloud computing, for example, has increasingly become an architectural problem for governments, as internet companies locate data beyond their reach, creating constraints on law enforcement, wiretap-

110. *See* Perlroth, *supra* note 107 (noting that some of the keys included in the database were "probably collected by hacking into companies' computer servers"). *See also* BUCHANAN, *supra* note 3, at 54–55 (describing a GCHQ hacking operation in which millions of encryption keys produced by Gemalto, a sim-card provider of many of hundreds of phone companies, were obtained by the agency).

111. *See*, *e.g.*, Ryan Gallagher, *Operation Auroragold: How the NSA Hacks Cellphone Networks Worldwide*, THE INTERCEPT (Dec. 4, 2014, 2:06 PM), https://theintercept.com/2014/12/04/nsa-auroragold-hack-cellphones/ [https://perma.cc/R4AN-WX2P] (explaining how the GSM Association hacking allowed "the NSA to track and circumvent upgrades in encryption technology used by cellphone companies to shield calls and texts from eavesdropping).

112. *See, e.g.*, BUCHANAN, *supra* note 3, at 64–76 (describing the NSA's alleged involvement in the creation and standardization of a backdoored encryption component known as Dual_EC, which the agency then encouraged and reportedly paid U.S. companies to implement in their products); Glen Greenwald et. al, *Microsoft Handed the NSA Access to Encrypted Messages*, THE GUARDIAN (July 12, 2013, 8:04 AM), https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data [https://perma.cc/WQ4R-JZVL] (describing collaboration between NSA and Microsoft that provided the agency with access to pre-encrypted data in servers storing data from some of the Company's services, including Outlook and Skype). *See also* Greg Miller, *The Intelligence Coup of the Century*, WASH. POST (Feb. 11, 2020), https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/ [https://perma.cc/QVW8-22QG] (detailing a U.S.-German collaboration with a Swiss firm called Crypto AG that was secretly owned by CIA and the German Federal Intelligence Service (BND). The story describes how the Company, which until liquidated in 2018, sold encryption devices to dozens of nations, and was in fact a well-orchestrated spying operation that gave the U.S. and German intelligence agencies (and, likely, their Five Eyes counterparts) access to the encrypted communications of their rivals. While the Company has lost its market power in the Internet era, the story reveals how far collaboration with information security firms can go).

113. *See* SHANE HARRIS, @WAR: THE RISE OF THE MILITARY-INTERNET COMPLEX 94–96 (2015) (describing how the software vulnerabilities market works).

ping and surveillance.[114] Government actions to circumvent this constraint have included enacting data localization laws[115] and collaborating with foreign governments to ensure access to data stored or generated abroad.[116]

To be sure, internet architecture remains a constraint on any government seeking to spy or hack for other purposes. Yet, many of the techniques once believed to keep governments outside private networks have been curtailed or avoided by massive campaigns to reassert government power over the World Wide Web. As the next section shows, this effort has not been only about playing defense; over the years, governments have come to realize that architecture is also an asset they can exploit and modify to their ends.

## B. Exploiting Architecture

> *"One of the things we see is that tools we've created, the tools you've created have been turned by others into weapons."*[117]

A key feature of the architecture of cyberspace is that not only does it constrain government cyber activity, but it also enables previously unattainable ways to collect and manipulate information.[118] Global connectivity promises to yield many economic and social opportunities to benefit mankind. Intel predicts that, by the end of the decade, 200 billion smart devices will be connected to the internet, with everyone having, on average,

---

114. Cloud service providers place their data centers based on optimization considerations featuring variables, including the costs of energy and land, local laws, geographic location, and more. *See* Andrew K. Woods, *Litigating Data Sovereignty*, 128 YALE L.J. 328, 347 (2018).

115. This is an example of what Lessig refers to as the "interconnectivity of constraints," the idea that by changing one constraint (the law), the government can modify another constraint (architecture). *See* LESSIG, CODE V. 2.0, *supra* note 14, at 123–24. Notably, laws restricting the transfer of data outside state borders make it more vulnerable to interception by the local government but purport to help keep data from falling into the hands of foreign governments. For this reason, legislative efforts to require local storage of personal data increased in the wake of the Snowden disclosures, when governments wanted to protect citizens from the NSA. Scholars are skeptical of the efficacy of data localization measures as part of an effort to counter foreign intelligence collection. *See* Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 715–18 (2015).

116. The U.S. for example, has clandestinely established data-sharing collaborations with Germany, Greece, Denmark, Saudi Arabia, and Bahamas. *See* BUCHANAN, *supra* note 3, at 30–33.

117. Brad Smith, President of Microsoft (quoted in in Steve Ranger, *Why Microsoft is Fighting to Stop a Cyber World War*, ZDNET (Dec. 12, 2018), https://www.zdnet.com/article/why-microsoft-is-fighting-to-stop-a-cyber-world-war/ [https://perma.cc/SG6P-RR8B]).

118. Accordingly, the public and academic discourse on the subject revolves around two competing narratives: one is the "going dark" metaphor mentioned above; the other is the characterization of the recent years as "the golden age of surveillance." *See* Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 420 (2012).

26 personal smart objects for daily use.[119] Sensors will measure nearly everything we do and record and feed back and forth a massive amount of data about us, our behavior, and our preferences.[120] However, the more things and the people using them get connected, the more opportunities there are for exploiting connectivity to spy, disrupt, and manipulate the data they aggregate and transmit, and the more harm that can be inflicted.[121]

The Internet of Things (IoT) and the rollout of the 5G network that will support it increase hacking-related risks and opportunities in two respects.[122] First, hacking objects with internet connectivity has the potential to create greater harm.[123] Taking control of or crippling software that helps people get information from computer screens is one thing, but when that software also controls infrastructure, medical equipment, power grids, and traffic lights, the consequences are not merely virtual, but also physical—and can be lethal.[124] Similarly, data collection that is not limited to computers and phones but extends to numerous other objects we use in our daily lives can be significantly more intrusive on privacy.[125]

Second, the sharp rise in the number of sensors and microphones around us means that, at nearly any given time, some application or object will record our behavior. Each added device on a network also provides a new point of entry to hostile actors seeking unauthorized access. A smart home environment, for example, will embed what is essentially eavesdropping technology in TVs, speakers, kitchen appliances, toys, AC systems, smoke detectors, security cameras, and many other devices, creating more ways than ever before to penetrate networks and collect personal information. In 2019, Microsoft provided a glimpse of the dangerous potential of IoT, when it uncovered an effort to target and compromise commonly used

119. INTEL, *A Guide to the Internet of Things: How Billions of Online Objects are Making the Web Wiser*, https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html [https://perma.cc/QA4U-W6GA].

120. *See generally* SAMUEL GREENGARD, THE INTERNET OF THINGS (2015); ROLF H. WEBER & ROMANA WEBER, INTERNET OF THINGS: LEGAL PERSPECTIVE (2010).

121. *See* LAURA DENARDIS, THE INTERNET IN EVERYTHING, 4 (2020) ("The stakes of cybersecurity rise as Internet outages are no longer about losing access to communication and content but about losing day-to-day functioning in the real world, from the ability to drive a car to accessing medical care"); *see also* Sara S. Beale & Peter Berris, *Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*, 16 DUKE L. & TECH 161, 163–68 (2017) (discussing security vulnerabilities in the IoT and explaining why the IoT is especially insecure).

122. *See* RICHARD A. CLARKE & ROBER K. KNAKE, THE FIFTH DOMAIN, 265–80 (2019).

123. *See* Beale, *supra* note 120 (discussing examples of attacks targeting IoT devices).

124. As the attack on the Iranian nuclear enrichment facility in Natanz proved a decade ago, the connectivity of industrial control systems provides new ways for nations to project state power. The operation utilized the Stuxnet malware to manipulate the control systems of the facility, stopping thousands of centrifuges form spinning.

125. DENARDIS, *supra* note 120, at 4; Jack M. Balkin, *Fixing Social Media's Grand Bargain*, 2 HOOVER INST. (2018) ("In general, the more interactive and the more social the service, the greater the opportunities for data collection, data analysis, and individualized treatment").

IoT devices to gain initial access to corporate networks.[126] The effort was attributed to "Strontium," also known as the Russian government hacking group "Fancy Bear."[127] Researchers in the company's Threat Intelligence Center discovered that the devices, which often feature simpler security configurations and weak security management, became "points of ingress from which the actor established a presence on the network and continued looking for further access."[128] This intrusion then compromised the entire network, as "[o]nce the actor had successfully established access to the network, a simple network scan to look for other insecure devices allowed them to discover and move across the network in search of higher-privileged accounts that would grant access to higher-value data."[129]

The threat, however, does not come only from foreign, state-sponsored entities. The mass accumulation of personal data by private entities is itself a cause for anxiety. Given what is now known about the role of private-public collaborations in developing mass surveillance programs, it should be kept in mind that these entities may voluntarily or be legally compelled to give access to government entities, and their servers and networks could be targeted by hackers, including government hackers.

The IoT is technological architecture that provides new pathways for surveillance and cyberattacks. Similarly, the shift to cloud-based products[130] and emerging technologies, such as deep fakes,[131] extends the range of actions malicious actors can take to collect and manipulate information. There is a legal dimension as well: when private data are stored in servers located abroad, as is often the case in cloud computing, accessing that data for purposes of foreign intelligence collection may be subject to less demanding legal constraints than had the data been stored locally.[132]

Taken together, these examples show how architecture, while imposing certain constraints on state cyber power, can also make governments more powerful in several new ways.

---

126. MICROSOFT SECURITY RESPONSE CTR., *Corporate IoT—A Path to Intrusion* (Aug. 5, 2019), https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/ [https://perma.cc/7V6T-HUS6].

127. Dan Goodin, *Microsoft Catches Russian State Hackers Using IoT Devices to Breach Networks*, ARS TECHNICA (Aug. 6, 2019), https://arstechnica.com/information-technology/2019/08/microsoft-catches-russian-state-hackers-using-iot-devices-to-breach-networks/ [https://perma.cc/HD2R-US9Y].

128. MICROSOFT SECURITY RESPONSE CTR., *supra* note 126.

129. *Id.*

130. *See* Berkman Ctr. Report, *supra* note 94, at 10 ("A service, which entails an ongoing relationship between vendor and user, lends itself much more to monitoring and control than a product, where a technology is purchased once and then used without further vendor interaction").

131. *See* Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CAL. L. REV. 1753, 1776–84 (surveying the harmful impact of deep fakes to society).

132. In the United States, for example, data of Americans collected incidentally overseas is not controlled by the authorization and oversight regime of the Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801–1813 (2015), but by the less constraining regime of Exec. Order No. 12,333, 3 C.F.R. 200 (1981).

## III. International Law

International law serves as a type of normative constraint on state power. The source of the sense of obligation to follow international law is disputed among scholars,[133] but as Professor Louis Henkin commented, "almost all nations observe almost all principles of international law and almost all of their obligations almost all of the time."[134] The constraining effect of international law operates on two different levels.[135] One is the international level, in which international law directs the behavior of nations in their relations with other nations and international organizations. Another is the domestic level. International law penetrates the domestic legal system in various formal and informal ways and exerts influence on the relationships between citizens and their government and among the branches of government.

Currently, the international law governing nonconsensual state interactions in cyberspace, as well as their implications for human rights, is in its infancy. So far, states have not been able or, perhaps, not willing to formulate new rules to regulate hostile cyber activities and manipulative uses of data. International efforts to clarify how existing law applies have failed to obtain consensus as well. This section considers how the current state of international law affects government power. It makes three main observations. First, offensive cyber activities that cross the use-of-force threshold or are carried out within the context of an existing armed conflict are regulated and constrained by international law. Second, there appear to be emerging soft law norms prohibiting some forms of cyber intrusion, such as economically motivated hacking. Third, there is a governance gap with respect to other types of cyber activities. This gap should not be understood simply as a lack of constraint, but rather as a source of empowerment for the state's executive branch.

### A. Governance Gaps in International Law

International law is developed formally around the mutual consent of states, created either by international practice (customary international law) or agreement (treaty law).[136] For cyberspace, there has been limited success in achieving wide acceptance of new law or clarifying the application of existing international law.

---

133. There are numerous theories of state compliance, but the core of the debate is whether states tend toward compliance because of instrumental or non-instrumental reasons. *Compare, e.g.*, JACK L. GOLDSMITH & ERIC A. POSNER, THE LIMITS OF INTERNATIONAL LAW (2009) (drawing from rational choice theory to conclude that states often comply with international law (and sometimes not) because it is in their rational self-interest) *with* THOMAS M. FRANCK, FAIRNESS IN INTERNATIONAL LAW AND INSTITUTIONS (1995) (arguing that the reason for compliance lies in the fairness and legitimacy of international rules).

134. LOUIS HENKIN, HOW NATIONS BEHAVE, 47 (2d ed., 1979) (emphasis omitted).

135. *See generally* John O. McGinnis & Ilya Somin, *Should International Law be Part of Our Law?*, 59 STAN. L. REV. 1175 (2007)

136. *See generally* MALCOLM N. SHAW, INTERNATIONAL LAW, 51–95 (8th ed., 2017).

We begin with what has been achieved so far. For more than two decades, concerns over the potential use of information and communication technologies (ICTs) for malign purposes have been on the agenda of the international community.[137] By the early 2000s, a growing number of states have acknowledged that cyberspace is becoming a new 'front' from which state and non-state actors can harm their national security. Since 2004, several U.N.-mandated groups of governmental experts (GGEs), with representatives from some of the most cyber-active nations, have been established to advance the global regulation of the cybersphere.[138] The five GGE processes concluded so far reflect a clear consensus: international law is applicable to cyberspace.[139] However, the member states did not agree on nearly anything else.[140] Ideological and geostrategic divides between East and West have been a major driver in the collapse of the Fifth GGE, leaving the state of play in a normative fog.[141] As of 2020, the international community is moving on two parallel tracks: one is a U.S.-led effort to continue the GGE process, with a Sixth group consisting of 25 members; the other is a Russian-led initiative known as the Open-Ended Working Group, that allows any interested U.N. member to participate in the meetings. This bifurcation of international negotiations indicates the

137. *See* AM. BAR ASS'N - PRIVACY & COMPUTER CRIME COMM., INTERNATIONAL GUIDE TO CYBER SECURITY, 82–85 (Jody R. Westby Ed., 2004) (describing international cyber security initiatives at the U.N. between 1990–2004).

138. G.A. Res. 58/32 (Dec. 8, 2003), 60/45 (Dec. 8, 2005), 66/24 (Dec. 2, 2011), 68/243 (Dec. 27, 2013), 70/237 ((Dec. 23, 1015), 73/266 (Dec. 22, 2018). For a summary of the U.N. GGE processes until late 2018, see Anders Henriksen, *The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace*, 5 J. CYBERSECURITY 1, 2-4 (2019). In addition, in 2019, the U.N. General Assembly established an open-ended working group acting on a consensus basis, an initiative sponsored by the Russian Federation. G.A. Res. 73/27 (Dec. 5, 2018).

139. Rep. of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 19, UN Doc. A/68/98 (June 24, 2013).

140. Note that the Fourth GGE (2014/15) made some additional vague pronouncements about the applicability of international law in cyberspace, conforming the duty of states to observe the principles of sovereignty, the settlement of disputes by peaceful means, and non-intervention, as well as obligations to "protect human rights and fundamental freedoms." Rep. of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 24–26, UN Doc. A/70/174 (Jul. 22, 2013).

141. Members of the Fifth GGE (20167/17) failed to agree on a draft for a consensus report. *See* Henriksen, *supra* note 138, at 3–4. What followed was a split between a U.S-led initiative to convene a Sixth GGE process and a Russian-led proposal to launch an open-ended working group to further develop common understanding of the law in this area, with each side pointing fingers at the other for distorting previous consensus resolutions. *See* G. A. First Comm., First Committee Approves 27 Texts, including 2 Proposing New Groups to Develop Rules for States on Responsible Cyberspace Conduct, GA/DIS/3619 (Nov. 8, 2018), https://www.un.org/press/en/2018/gadis3619.doc.htm [https://perma.cc/6TEK-NT8P]. Commentators have argued that the failure of the fifth GGE to produce a consensus report inspired a trend among states to shift away from law-making or law-clarifying efforts to developing voluntary norms outside the confines of the law. *See, e.g.*, Kubo Maèák, *Is the International Law of Cyber Security in Crisis?*, 130–31 in 8TH INT'L CONF. ON CYBER CONFLICT: CYBER POWER (Maj N. Pissanidis et al, eds., 2016).

lack progress in creating or clarifying the law.[142]

Various non-state actors have filled the vacuum left by states' inability to clarify how specific international legal norms apply to cyberspace and have launched their own law-clarifying initiatives.[143] The most prominent of these is the Tallinn project, a working group of international experts convened in Tallinn, Estonia under the auspices of the NATO Cooperative Cyber Defense Center. The Tallinn group of experts drafted two comprehensive manuals (2013, 2017), on a range of inter-state cyber activities, aiming to articulate and interpret existing law, rather than suggesting new law.[144] Most states, however, have been reluctant to bind themselves, and have positively accepted the positions set forth in the manuals.[145] In a study that analyzed the responses of victim states to cyberattacks, Dan Efrony and Yuval Shany found only "limited support in state practice for certain key [Tallinn] rules" and concluded that states with large footprints in cyberspace appear content with the ambiguous state of the law.[146] Their study supports the conclusion that many fundamental normative issues remain in a state of flux. To be sure, this void encompasses not only norms governing state-to-state relations but also broader issues. For example, unlike conventional arms trade, which is subject to an international treaty regime, cyber weapons trade is largely unregulated at the international level, leaving vague legal boundaries for a thriving private hacking industry.[147]

This description is not meant to suggest that there is a *non liquet*—a situation of no law at all—in cyberspace. When cyber operations exceed a certain level of harm, it is widely accepted that they are regulated by international law on the use of force (*jus ad bellum*) and the conduct of hostilities (*jus in bello*).[148] Moreover, recent state practice suggests the

142. *See, e.g.*, Elaine Korzak, *What's Ahead in the Cyber Norms Debate?*, LAWFARE (Mar. 16, 2020, 12:08 PM), https://www.lawfareblog.com/whats-ahead-cyber-norms-debate [https://perma.cc/FBK8-BJYJ].

143. *See, e.g.*, MICROSOFT, International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World (2015); Int'l Comm. Red Cross, International Humanitarian Law and Cyber Operations during Armed Conflicts (2019).

144. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013); TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2017) [hereinafter, TALLINN MANUAL 2.0].

145. *See, e.g.*, Paul C. Ney, Jr., DOD General Counsel Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020) (noting that "[i]nitiatives by non-governmental groups like those that led to the Tallinn Manual can be useful to consider, but they do not create new international law, which only states can make").

146. Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice*, 112 AM. J. INT'L. L. 583 (2018).

147. *See* Human Rights Council, Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Surveillance and Human Rights, UN Doc. A/HRC/41/35 (May 28, 2019), at 11–12 [hereinafter, *Special Rap. Rep. on Digital Surveillance*] (describing the difficulties in applying the arms export control regime to cyber technologies).

148. For *jus ad bellum* restrictions on cyber activity, see TALLINN MANUAL 2.0, *supra* note 144, Rules 68–70; Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 841–49 (2012); Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back*

emergence of a norm banning economically motivated hacking, that is, cyber espionage for the benefit of businesses.[149] There is a legal gap beyond these limited regulations. This "gap" occupies the gray areas of conflict and competition, a broad spectrum of hacking and surveillance activities below the use-of-force threshold that nonetheless harm the victim state. In theory, there are other rules of international law that impose constraints on state cyber activity, but the reality is that they are toothless, for three main reasons.

First, this sort of hostile cyber activity falls between the cracks. While there are several relevant legal paradigms, including the principles of sovereignty and non-intervention, it is far from clear if they are triggered by—and how they would be applied to—a broad range of cyber operations.[150] The non-intervention principle prohibits only acts that include an element of coercion, defined as a behavior that deprives the targeted state of free choice over its sovereign functions.[151] As cyber intrusions often do not

---

*to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421 (2011); Yoram Dinstein, *Computer Network Attacks and Self-Defense*, 76 INTL' L. STUD. 99, 102–04 (2002). Note, however, that the threshold for what constitutes "use of force" is unsettled. Some states insist that only cyberattacks that produce physical damage or that injure or kill persons meet the threshold. *See, e.g.*, Jeremy Wright, the U.K. Attorney General, Speech Delivered at Chatham House, London: Cyber and International Law in the 21st Century (May 23, 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century [PERMA]. Others adopt a broader view, according to which cyber acts causing significant economic or financial consequences are also covered by the prohibition. *See, e.g.*, France Ministry of the Armed Forces, International Law Applicable to Operations in Cyberspace (Sept. 9, 2019) (in French). Still others, like China, refuse to clearly state their position but seem to prefer an exceptionally narrow application of the use of force paradigm to cyber activities. *See* Julian Ku, *How China's Views on the Law of Jus ad Bellum Will Shape Its Legal Approach to Cyberwarfare*, 2–4 HOOVER INST. (Aug. 17, 2017).

The application of *jus in bello* (also, international humanitarian law, IHL) principles to cyber is supported by, among others, the United States., The Netherlands, The U.K., France, The EU, NATO and the ICRC, but has been challenged by China. *See* Michael Schmitt, *The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis*, JUST SECURITY (Oct. 14, 2019), https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/ [https://perma.cc/59TB-X6E2] (surveying states' *opinio juris* on the applicability of IHL to cyber operations). Here too, however, the devil is in the details, as the application of some of the core IHL principles to the cyberwar theater proves difficult. *See generally* Jack Goldsmith, *How Cyber Changes the Laws of War*, 24 EU. J. INT'L L. 129 (2013).

149. The norm was first articulated by the Obama administration in Presidential Policy Directive (PPD) 28. *See* Office of the Press Sec'y, PPD on Signals Intelligence Activities, White House § 3(c) (Jan. 17, 2014) [*hereinafter* PPD 28] (prohibiting collection for the purpose of affording "a competitive advantage to U.S. companies and U.S. business sectors commercially"). In recent years, the norm has garnered wide acceptance in bilateral and multilateral agreements. *See, e.g.*, Samuel J. Rascoff, *The Norm Against Economic Espionage for the Benefit of Private Firms: Some Theoretical Reflections*, 83 U. CHI. L. REV. 249, at notes 8–10 (2016); Asaf Lubin, *The Liberty to Spy*, 61(1) HARV. INT'L L.J. 185, 239–41 (2020).

150. For a comprehensive analysis of these paradigms in the context of hostile cyber operations, see Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention*, CHATHAM HOUSE (Dec. 2019); TALLINN MANUAL 2.0, *supra* note 144, at Rules 1–5, 66.

151. The prohibition of intervention is recognized as a norm of customary international law. *See generally* Philip Kunig, *Intervention, Prohibition of,* MAX PLANCK ENCYCLO-

clearly satisfy the coercion requirement[152]—either because they are merely disruptive,[153] or because they target individuals and private entities[154]—the principle is rarely implicated. Invoking the principle of sovereignty is even more in dispute. There are two competing views on the status of sovereignty in international law: in one view, sovereignty is not a binding rule of law but rather a guiding principle from which specific legal norms, such as the prohibitions on the use of force and intervention, derive, and, therefore, sovereignty does not prohibit cyber intrusions per se.[155] In the other view, sovereignty is a primary rule of law,[156] albeit an exceptionally vague one, since states have rarely expressed opinio juris on its meaning.[157] Either way, it is impossible to identify with certainty the point at which a cyber operation becomes a wrongful act. Cyber espionage and the theft of personal data, for example, are not clearly outlawed.[158]

Second, and relatedly, international law, by its very nature, deals poorly with normative uncertainty. The legal gaps and ambiguities addressed above would not have been a serious obstacle had international

---

PEDIA OF PUBLIC INT'L LAW (2008)). As articulated by the ICJ in the *Nicaragua* case, to qualify as an unlawful intervention in the affairs of another state, an act must be coercive and implicate matters subject to the sovereign authority of the targeted state, including the "the choice of a political, economic, social and cultural system, and the formulation of foreign policy." Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) (Nicaragua), 1986 I.C.J. Rep. 14, ¶ 205.

152. There is no universally accepted definition of coercion. Specifically, commentators disagree on the required intensity level of the coercive conduct, with definitions varying between acts that are "dictatorial" or "forcible" in nature to acts that merely deprive the state of control over a matter under its sovereign authority. *See generally* Sean Watts, *Low-Intensity Cyber Operations and the Principle of Non-Intervention*, in CYBER WAR: LAW & ETHICS FOR VIRTUAL CONFLICT, 249 (Jens D. Ohlin et. al. eds., 2015). In the cyber context, the Tallinn group of experts was divided over several aspects of the coercion requirement. *See* TALLINN MANUAL 2.0, *supra* note 144, at 317–25.

153. An example is political doxing. The most famous political doxing incident has been the Russian-led hacking into the computers of the Democratic National Committee (DNC) and the subsequent release of e-mails months before the 2016 presidential election. For analysis of the DNC hack under international law, see Jens D. Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEX. L. REV. 1579 (2017) (arguing that "the notions of 'sovereignty' and 'intervention'—though mainstays of contemporary public international law doctrine—are poorly suited to analyzing the legality [of the DNC hack]"; Ido Kilovaty, *Doxfare*, 9 HARV. NATL. SEC. J. 146, 169 (2018) (noting that "the current law on non-intervention is unsatisfactory when applied to doxfare").

154. Note, however, that attacks against private actors, carried out in order to compel state authorities to act or refrain from acting in a certain way, may still violate the non-intervention principle. *See* TALLINN MANUAL 2.0, *supra* note 144, at 315–316.

155. *See, e.g.*, Wright, *supra* note 148; Brian J. Egan, Legal Adviser, U.S. Dep't State, Remarks on International Law and Stability in Cyberspace, Berkeley Law School, California (reprinted in 35 BERKELEY J. INT'L LAW. 169 (2017); Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AM. J. INT'L L. UNBOUND 207 (2017).

156. *See, e.g.*, TALLINN MANUAL 2.0, *supra* note 144, at 21. For the difficulty in ascertaining the threshold for what constitute a violation of state sovereignty, see Moynihan, *supra* note 150, at 21, 23.

157. *See* Minister of Foreign Affairs, Letter to the Parliament on the international legal order in cyberspace (Jul. 5, 2019) [the Netherlands]; *see also* France Ministry of the Armed Forces, *supra* note 148.

158. *See* TALLINN MANUAL 2.0, *supra* note 144, at Rule 32.

law featured the institutional apparatus to resolve them and coerce compliance, if needed. As conceptualized by H.L.A. Hart, international law is an ill-developed legal system because it lacks crucial "secondary rules" to establish the content and meaning of the law.[159] The absence of centralized legislative and judicial institutions to promulgate rules and resolve disputes allows states a great deal of room to maneuver when there are reasonable disagreements about how the law applies to new circumstances, e.g., with relation to cyberspace. As commentators have noted, there are good reasons to rethink the coercion element, including to vindicate the values underlying the non-intervention principle in the cyber domain.[160] However, because non-intervention is a norm of customary international law, commissioning a binding change is extremely difficult. In order to establish opinio juris, there must be widespread state practice, with convincing evidence that it is carried out with a sense of legal obligation .[161] As a result, the process for changing customary international law is inherently uncertain—and its outcome can virtually always be disputed.

Finally, there is the *Lotus* principle.[162] The principle articulated by the Permanent Court of International Justice in the *Lotus* case—that, in the absence of a positive legal prohibition, states enjoy a presumption of legality in exercising their sovereign authority—although controversial, remains a meta-principle of international law. In the cyber context, the *Lotus* principle means that genuine uncertainty about whether a matter is regulated by international law will redound to the benefit of the state.[163] Therefore, cyberattacks, which do not clearly fall within one of the categories that restricts states' freedom of action, will be presumptively legal. Accordingly, the costs that states incur from violating partly acceptable norms of behavior will be minimal, if at all.

For all these reasons, when states contemplate taking hostile action in cyberspace, but below the use-of-force threshold, international law can do little to inhibit them. On the flipside, international law provides insufficient remedies for states suffering cyberattacks. From a strategic perspective, this state of affairs encourages states to exceed common boundaries and not commit to legal positions that might run contrary to their foreign policy interests.[164] From a normative perspective, this has implications for the domestic separation of powers, as the next section explains.

159. H.L.A. HART, THE CONCEPT OF LAW, 92–98, 213–237 (2D ED., 1994). *See also* LOUIS HENKIN, HOW NATIONS BEHAVE 22–25 (2d ed., 1979). Scholars have used international law's institutional and procedural limitations as an argument to question its status as "real law". I advance no such argument. My goal is merely to explain why states enjoy a relative high degree of flexibility in pursuing their security and foreign policy objectives in cyberspace.

160. *See, e.g.*, Ido Kilovaty, *The Elephant in the Room: Coercion* 113 AJIL UNBOUND, 87 (2019); Watts, *supra* note 152.

161. *See generally* GOLDSMITH & POSNER, *supra* note 133, at 23–24.

162. S.S. Lotus (Fr. v. Turk.), 1927 PCIJ (ser. A) No. 10, (Sept. 7, 1927), at 18–19.

163. I stress "genuine" because otherwise it might be mistakenly understood that any legal uncertainty might give rise to a presumption that states have liberty to act. *See* Martti Koskenniemi, *The Politics of International Law*, 1 EU. J. INT'L L. 4, 18 (1990).

164. *See* Efrony & Shany, *supra* note 146.

B. International Cyber Law as a Constraint (and Empowerment)

As mentioned earlier, international law influences the domestic legal system in numerous ways. International law may be incorporated into the domestic legal system and become part of domestic law;[165] it may be internalized in the system indirectly, for example, in rules of statutory construction requiring that statutes be construed, so far as reasonably possible not to violate international law;[166] it may serve as a guiding interpretive principle, that is, a tool that helps understand the meaning of domestic law;[167] and it may be grafted on a nation's case-law by judicial decisions that treat customary international rules as part of the "common law."[168] Different institutions may facilitate the role of international law in the domestic legal system, including the national constitution, the legislative process, judicial decisions, and unwritten conventions and customs.

The domestic legal effects of international law are a constraint, in the sense that they regulate the relationships between domestic actors. In *Big Brother Watch v. the United Kingdom*, the European Court of Human Rights found aspects of Britain's mass surveillance program in violation of articles 8 and 10 of the European Convention on Human Rights (ECHR), in part because the law authorizing the program lacked adequate mechanisms for independent oversight.[169] The decision drew on the ECHR, an instrument of international law, to limit the power of the British government to tap into the online communications of its citizens and to require greater independent oversight of executive action. Notice how international law inserted itself into two sets of relationships regularly governed by a nation's domestic public law: (1) the decision to limit the authority for mass collection concerns the relationship between the citizens and their government; (2) the decision to require the British government to introduce a more robust oversight system affects the relationships among the branches of government and its organizing principle: the separation of

165. Nations use a variety of institutional mechanisms for incorporating international law in the domestic legal system. In legal theory, a nation's approach to the role of international law in the domestic legal system is often described in terms of the monist-dualist distinction. In monist legal systems, international law is automatically part of state law and, subject to conflict rules, may override or displace domestic law. In dualist legal systems, a formal act of incorporation is required for international law to receive the status of law in the domestic legal system. Scholars have shown that, most nations do not adopt a monolithic approach but rather combine elements of both theories. *See* Pierre-Hugues Verdier & Mila Versteeg, *International Law in National Legal Systems: An Empirical Investigation*, 211–13, in COMPARATIVE INTERNATIONAL LAW (Anthea Roberts et al. Ed., 2018).

166. *See, e.g.*, Murray v. Schooner Charming Betsy, 6 U.S. (2 Cranch) 64 (1804).

167. *See* Roper v. Simmons, 543 U.S. 551 (2005) (using international and foreign law materials to interpret the U.S. Constitution). *See also* Sarah H. Cleveland, *Our International Constitution*, 31 YALE J. IN'L. L. 1 (2006) (examining the role of international law in constitutional analysis).

168. *See, e.g.*, HCJ 769/02 The Pub. Comm. Against Torture in Israel v. Gov't of Israel, (Dec. 14, 2006) (invoking customary international law rules to develop a judge-made norm on the practice of targeted killing of suspected terrorists).

169. Big Brother Watch v. The U.K., App nos. 58170/13, 62322/14 and 24960/15 (2018).

powers.[170] For both sets of relationships in this example, international law constrained executive power.

However, as foreign relations law scholars have shown in other contexts, international law sometimes enhances rather than constrains executive power.[171] The nature of the interaction between international law and the domestic legal system is such that legal authority to act under the former can be invoked in different ways to extend legal authority under the latter. In other words, compliance with international law provides a certain measure of legitimacy to a desired course of action, and that legitimacy can be used to compensate for weak legal arguments under domestic law, or to interpret domestic law to enable the course of action. This is especially significant because the Executive typically has more control over the development of international law than over the development of domestic law. In the long run, assertions of power justified under international law may empower the Executive at the expense of the other branches.

For example, the international law governing attribution of an internationally wrongful act has many loose ends. It lacks evidentiary rules necessary to establish state responsibility and does not clearly state the procedure for legal attribution or what level of publicity is required.[172] As a result, the Executive retains flexibility on how and when it makes attributions for cyber incidents. Under domestic law, however, an act of attribution triggers a host of legal justifications for measures against other state and possibly non-state actors. In the case of the United States, as Kristen Eichensehr has recently shown, it empowers the President to act, pursuant to his Art. II authority and, under specific legislation, against certain actors.[173] It follows that the limited regulation of what constitutes legal

170. For the role of international law in separation-of-powers debates, see Jean Galbraith, *International Law and the Domestic Separation of Powers*, 99 VA. L. REV. 987, 990 (2013) ("As it turns out, historically both political branches have relied on international law as an interpretive principle for determining the boundaries of their constitutional powers").

171. *See* Rebecca Ingber, *International Law Constraints as Executive* Power, 57 HARV. INT'L L. J. 49 (2016) (describing "mechanisms through which the executive invokes international law as a means of enhancing domestic power"); Curtis A. Bradley & Jean Galbraith, *Presidential War Powers as an Interactive Dynamic: International Law, Domestic Law, and Practice-Based Legal Change*, 91 N.Y.U. L. REV. 689, 761 (2016) ("presidents have drawn from international law to enhance their domestic authority to use force"); Galbraith, *supra* note 170, at 1008 ("Importantly, rather than being neutral, the influence of international law has typically served to strengthen the President's powers vis-à-vis Congress"); Cleveland, *supra* note 167, at 23–26 (describing how international law has been employed by courts to displace the applicability of domestic legal constraints).

172. *See* Eichensehr, *Cyberattack Attribution*, *supra* note 60, at 559 ("International law is unclear on the standard of proof that states must meet when accusing other states of internationally wrongful acts"); Michael N. Schmitt & Yuval Shany, *An International Attribution Mechanism for Hostile Cyber Operations?* 96 INT'L L. STUD. (forthcoming, 2020), available at SSRN: https://ssrn.com/abstract=3628435 [https://perma.cc/JKT3-PFBP] (noting that "the responsibility to release the evidence underlying attribution was styled [by the 2015 GGE] a voluntary, non-binding norm of responsible state behavior, not a legal obligation").

173. *See* Kristen E. Eichensehr, *Cyberattack Attribution as Empowerment and Constraint*, HOOVER INST. (2021).

attribution under international law provides wiggle room for the Executive to assert broad authority under domestic law. This example reflects a broader dynamic: an international law regime in early stages of its development affords some flexibility to states on what is permissible and how to categorize actions–as uses of force, countermeasures, acts of espionage, political acts, etc. This flexibility usually serves the Executive, who is able to maneuver strategically in ways that bolster its authority under domestic law. Over time, such invocations of international law authority may establish precedents that will down the road be relied upon as "historical practice," an independent source of domestic legal authority.[174]

## IV. International Politics

International politics is another element regulating government behavior in cyberspace. There is nothing new or controversial in the idea that states act on the international plane based on pressures from, interactions with, and power relative to other states. The rise of the digital sphere as a venue of geopolitics, however, creates new conditions for the management of state-to-state interactions. These conditions challenge some of the fundamental assumptions underlying international relations theory of the pre-digital era.[175] This Part identifies two sources of constraint from international politics that are unique to cyber: one arising from the relative multipolarity of the international cybersecurity environment; another arising from recent tensions surrounding data transfers. These constraints do not impact all states equally.

### A. Constraints arising from a Multipolar Cybersecurity Environment

International relations scholars use the concept of polarity to describe the distribution of power in the international system.[176] The "poles" refer to the number of great powers, at any given period, that compete for hegemony and influence over the world order. The post-Cold War distribution of power has been recognized as a unipolar system, in which one country, the United States, surpasses all others in military, economic, and cultural power.[177] In a unipolar world, the one superpower faces very few

174. Indeed, scholars have analyzed the growth in presidential war powers in U.S. law under this conceptual frame. *See, e.g.*, Galbraith, *supra* note 170, at 1019–27. As she explains, during the 19th and early to mid-20th centuries, presidents have resorted to *international law* to support the proposition that they are *constitutionally* entitled to use military force without legislative approval, in cases when doing so served a vital U.S. interest. Over time, uses of force originally justified by international law have become an established constitutional practice, removed from their international law roots and unable to account for the developments in this body of law.

175. *See generally* Nazli Choucri, *Explorations in Cyber International Relations: A Research Collaboration of MIT and Harvard University*, MIT Political Science Department Research Paper No. 2016-1, available at SSRN: https://ssrn.com/abstract=2727414 [https://perma.cc/VZ8Y-4GST].

176. *See generally* KENNETH N. WALTZ, THEORY OF INTERNATIONAL POLITICS (1979); UNIPOLAR POLITICS (Ethan B. Kapstein and Michael Mastanduno eds., 1999).

177. Charles Krauthammer, *The Unipolar Moment*, FOREIGN AFFAIRS (1990/91).

constraints in its pursuit of national security and international goals.[178]

The assumption of unipolarity is significantly challenged in cyberspace. The United States and its Western allies are still the dominant powers in the virtual domain,[179] but (1) the gap in cyber power between them and rival states and non-state actors is much smaller and (2) the United States is more vulnerable.[180] What accounts for the relative weakness of the United States vis-à-vis its adversaries? International relations scholarship identifies four main factors.

First is the nature of international competition in cyberspace. While early predictions about how cyber wars would be fought were apocalyptic—large-scale attacks resulting in catastrophic impact on an entire country[181]—what actually transpired were daily engagements of state and non-state actors hacking for limited geopolitical gains.[182] Espionage, data theft, doxing (i.e., the unauthorized publication of private materials), temporary disruption, subversion, and other low-intensity intrusions do not trigger legal authorities to sanction the use of physical force in retaliation. Powerful democracies are then left with no tools to deter and punish hostile acts.[183] As one commentator noted, the fact that cyber operations are "hard to see and left little blood" makes it difficult "for any country to muster a robust response."[184] It is ultimately for states to articulate the contours of what is or is not acceptable in cyberspace. For the time being, at least, the West does not appear willing or able to authorize forceful countermeasures.[185]

Second is the problem of attribution. Identifying the source of an attack is critical in cyber defense at various levels: operational (strengthening cyber resilience), diplomatic (naming and shaming perpetrators), and legal (enabling countermeasures under international law and individual

178. *See* Daniel Abebe, *Great Power Politics and the Structure of Foreign Relations Law*, 10 CHI. INT'L L.J. 125, 133 (2009).

179. *See* Belfer Ctr. - Harv. Kennedy School, National Cyber Power Index 2020, at 20–25 (Sept. 2020), https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf [https://perma.cc/KNX6-VJ4L].

180. Joseph S. Nye Jr., *Cyber Power*, BELFER CTR. - HARV. KENNEDY SCHOOL, 9 (2010) (arguing that "the diffusion of power in the cyber domain is represented by the vast number of actors, and relative reduction of power differentials among them").

181. Policymakers and commentators often use metaphors such as "cyber-Pearl Harbor," "cyber 9/11," and "cyber-Katrina" to frame the threat. *See*, *e.g.*, Remarks by U.S. Secretary of Defense Leon E. Panetta on Cybersecurity to the Business Executives for National Security (Oct. 11, 2012), https://content.govdelivery.com/accounts/USDOD/bulletins/571813 [https://perma.cc/3QMQ-SQXQ] (warning about a looming "cyber-Pearl Harbor").

182. *See generally* BUCHANAN, *supra* note 3; SEAN T. LAWSON, CYBERSECURITY DISCOURSE IN THE UNITED STATES: CYBER-DOOM RHETORIC AND BEYOND (2020).

183. Two of the most common tactics used by victim states— "naming and shaming" and indicting individual perpetrators—have been found by commentators to be largely ineffective in promoting accountability or deterrence. *See*, *e.g.*, Mark Pomerleau, *Why the US Chose to 'Name' and 'Shame' Russia over Cyberattacks*, FIFTH DOMAIN (Feb. 20, 2020), https://www.fifthdomain.com/international/2020/02/21/why-the-us-chose-to-name-and-shame-russia-over-cyberattacks/ [https://perma.cc/P68Y-EA2U].

184. SANGER, *supra* note 5, at 169.

185. BUCHANAN, *supra* note 3, at 317.

indictments). It is also problematic, with technical, forensic, legal, and political difficulties.[186] In recent years, attributions have turned into a cat-and-mouse game between analysts and hackers, as sophistication and skill have grown on both sides. For example, the hackers who carried out the 2018 Winter Olympics attack have used various means of deception known as false-flags to lead investigators in many different directions, generating confusion and doubt.[187] Years later, the identity of the state behind this attack is still disputed.[188] To take another example, the Wiper attack on Iran's oil ministry used a code that after destroying the target system immediately destroyed itself, leaving little evidence that an attack had even occurred.[189] Not knowing with sufficient certainty who initiated an attack, for what purpose, and where the attack originated allows the perpetrator plausible deniability and impedes the efforts to set clear red-lines.[190] In this chaotic environment, it is harder for the powerful parties to create and maintain deterrence.

Third, democratic states are relatively more constrained and vulnerable.[191] Some of the values that form the backbone of democratic societies—free press, free elections, the right to privacy, rule of law and others—impose limitations on what democratic governments can do in cyberspace, producing more opportunities for adversaries to exploit.[192] In recent years, countries like Russia, North Korea, and Iran have skillfully used the lack of governmental control of the media, to increase the impact of their operations against the West and exploited social media, to sow division and undermine trust in democratic institutions. In addition, the strict separation between the public and private sectors limits governmental presence in private networks, which, in turn, constrains the robustness of cyber defensive and offensive capabilities.[193] On average, Western societies are also more dependent on digital networks, which makes them more

186. For the technical and forensic aspects of the attribution problems, see W. Earl Boebert, *A Survey of Challenges in Attribution*, in Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy 43–48 (2010); Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38 J. STRATEGIC STUD., 8–14 (2015). For the legal aspects, see Eichensehr, *Cyberattack Attribution*, *supra* note 60, at 559–87.

187. *See* Andy Greenberg, *The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History*, WIRED (Oct. 17, 2019, 6:00 AM), https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/ [https://perma.cc/TLB9-RR8D].

188. *Id.*

189. BUCHANAN, *supra* note 3, at 143–44. *See also* Kim Zetter, *Wiper Malware That Hit Iran Left Possible Clues of Its Origins*, WIRED (Aug. 29, 2012, 9:00 AM), https://www.wired.com/2012/08/wiper-possible-origins/ [https://perma.cc/369B-HKUX].

190. *See* Joseph S. Nye Jr., *Deterrence and Dissuasion in Cyberspace*, 41 INT'L SEC., 44, 49–52 (2017).

191. For a comprehensive analysis (as applied specifically to the United States), see Goldsmith & Russel, *supra* note 16, at 4–15.

192. *Id.*, at 9–11 (arguing that various types of cyberattacks are more effective when employed against free and open societies).

193. *See* SANGER, *supra* note 5, at 78–99 (describing the efforts of tech giants Google and Apple in withholding access to their servers and devices from U.S. intelligence and law enforcement agencies).

exposed to malicious attacks. Escalation, in this logic, would be more harmful to them than to less digitally dependent nations.

Finally, there is the accessibility of cyber weapons. Unlike warplanes and nuclear missiles, cyber weapons are relatively inexpensive to develop, quick to deploy, and easy to deny. North Korea, for example, has developed one of the most aggressive and effective military cyber programs, despite its diplomatic isolation and economic hardship.[194] As malicious codes can be mutated and redeployed rather easily, the increase in cyberattacks in and of itself contributes to the proliferation of cyberweapons.[195] A study found that between 2001 and 2017, the number of states that created military cyber units rose from 5 to 63.[196] One year later, the former deputy director of the NSA estimated that the number of nations capable of mounting cyberattacks grew to more than 100.[197]

These features of the cyber arena enable weaker states and non-state actors to shift the balance of power in their favor. In this relatively multipolar environment, the powerful states, and liberal democracies in particular, face significant new political constraints on using cyber force and retaliating against attacks and provocations.[198] In a series of articles, Daniel Abebe argued that there is (and should be) a relationship between the structure of constraints generated by international politics and the level of domestic legal constraints imposed on the government.[199] As the shift from a unipolar to a multipolar international system increases the level of political constraint, disregarding the relationship may result in overconstraint, undermining the capacity of democratic governments to compete successfully in cyberspace.[200] According to this line of argument, we can view laws regulating war and foreign affairs powers in the United States as devices that, in a unipolar world, function to curb the risk of unnecessary wars (this risk is high, arguably, because there are relatively little geopoliti-

194. *See, e.g.*, SANGER, *supra* note 5, at 124–51; *see also Cyber Operations Tracker*, Democratic People's Republic of Korea, COUNCIL ON FOREIGN REL., https://www.cfr.org/interactive/cyber-operations#Takeaways [https://perma.cc/9BLD-VH36].

195. Daniel Cohen & Aviv Rotbart, *The Proliferation of Weapons in Cyberspace*, 5 MILITARY AND STRATEGIC AFFAIRS, 59, 62 (2013).

196. Anthony Craig, *Understanding the Proliferation of Cyber Capabilities*, COUNCIL ON FOREIGN REL. (Oct. 18, 2018), https://www.cfr.org/blog/understanding-proliferation-cyber-capabilities [https://perma.cc/L2QG-MQUM].

197. Mike Levine, *Russia Tops List of 100 Countries that Could Launch Cyberattacks on US*, ABC NEWS (May 18, 2017, 6:54 PM), https://abcnews.go.com/US/russia-tops-list-100-countries-launch-cyberattacks-us/story?id=47487188 [https://perma.cc/QHU2-3KH8].

198. For examples, see SANGER, *supra* note 5, at 100–170.

199. Abebe, *supra* note 17; Abebe, *supra* note 178. *See also* Robert Knowles, *American Hegemony and the Foreign Affairs Constitution*, 41 ARIZ. ST. L.J. 87, 128–29 (2009) (arguing that in a unipolar world, U.S. courts should be less deferential to the President's foreign affairs decision-making).

200. *See* Daniel Abebe, *Cyberwar, International Politics, and Institutional Design*, 83 U. CHI. L. REV. 1, 2 (2016) ("a framework that does not consider the complex relationship between the two types of constraints might result in a regulatory regime that leaves the president overconstrained and unable to achieve [U.S.] cyberpolicy goals").

cal costs and constraints).[201] However, this risk is already mitigated in cyberspace because it is not unipolar. Abebe's logic may lead to the conclusion that the United States and its allies are sufficiently constrained by the new balance of cyber power. As far as it goes, this is a valid argument. However, it is insufficient under the framework adopted in this Article. One must also account for the constraint and empowerment generated by the other forces of cyberspace—including international law, architecture, and the private sector—to draw normative conclusions on the appropriate level of legal constraint on the government.

B. Constraints arising from Data Transfers Disputes

International data transfers are an essential feature of the global digital economy.[202] A recent Congressional report notes that "data flows enable people to transmit information for online communication, track global supply chains, share research, provide cross-border services, and support technological innovation."[203] Data transfers between the United States and the E.U. alone affect more than 5,000 businesses and serve a "$7.1 trillion transatlantic economic relationship."[204] But as data travels around the globe, a clash between competing powers whose interests are involved is inevitable. One such recent clash showed how states can leverage control over their data to impose constraints on other states.

Major responsibility for the trend to restrict data transfers rests with Edward Snowden. One of Snowden's many scandalous exposures was the depth of the relationship—voluntary and compelled—between the NSA and American communications and technology firms.[205] The leaks revealed that, by leveraging corporate partnerships and relying on broad legal authorities compelling U.S. providers to produce data upon request, the U.S. government for years engaged in mass surveillance of internet and telephony communications around the globe. As a legal matter, what made this surveillance more alarming to many was that U.S. law provided foreigners with far less protection from surveillance than U.S. persons.[206] Post-Snowden, trust in both the U.S. government and the culpable firms

201. *See generally* Monica Hakimi, *Techniques for Regulating Military Force*, 735-52 in THE OXFORD HANDBOOK OF COMPARATIVE FOREIGN RELATIONS LAW (Curtis A. Bradley ed., 2019).

202. *See* Joshua Meltzer & Peter Lovelock, *Regulating for the Digital Economy*, BROOKINGS INST. 1-9 (2018).

203. Cong. Research Serv. IF11613, U.S.-EU Privacy Shield (Aug. 6, 2020).

204. U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows (July 16, 2020).

205. *See* Ewen MacAskill & Dominic Rushe, *Snowden Document Reveals Key Role of Companies in NSA Data Collection*, GUARDIAN (Nov. 1, 2013, 9:40 PM), https://www.theguardian.com/world/2013/nov/01/nsa-data-collection-tech-firms [https://perma.cc/65DQ-7UZL]. One of the leaked presentations laid bare the goal of this relationship: "Leverage unique key corporate partnerships to gain access to high-capacity international fiber-optic cables, switches and/or routes throughout the world." *Id.*

206. *See* The President's Review Grp. On Intelligence and Commc'ns Techs., Liberty and Security in a Changing World, 64 (2013) ("the President has broad constitutional authority to protect the nation in the realm of foreign intelligence surveillance without complying with the usual requirements of the Fourth Amendment").

has been severely damaged.[207] Europe, in particular, sought explanations and legal or policy reforms that would align the United States more closely with European data protection standards.[208] In 2014, these pressures, which included voices calling to restrict transatlantic data transfers,[209] yielded some changes in U.S. signals intelligence collection policy.[210] But notwithstanding initial hype, the changes were modest and did not impose significant constraints on the intelligence community.[211] Despite the outcry, Europe seemed to lack the leverage to force the United States into meaningful limitation of its intelligence collection practices.

But where traditional diplomacy fell short, EU data protection law and institutions stepped in. Exporting personal data from the EU is subject to stringent requirements for privacy protection.[212] The receiving party must provide sufficient assurances that data are adequately protected from breaches, leaks, and prying eyes, including those of local government. This often requires negotiations between the EU and the receiving state, in which the latter's privacy laws, general adherence to the rule of law, and human rights record are vetted according to European standards.[213] Until 2015, transatlantic data transfers were in compliance with EU law under a framework known as the Safe Harbor Privacy Principles, negotiated by the parties and approved by the European Commission.[214] In *Schrems v. Data Protection Commissioner (Schrems I)*, the European Union Court of Justice (CJEU) ruled in favor of an Austrian national who argued, based on the Snowden leaks, that personal data in his Facebook account was not adequately protected from U.S. government surveillance.[215] The decision, invalidating the Safe Harbor scheme, prompted new negotiations that

207. *See, e.g.*, Claire C. Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES (Mar. 21, 2014), https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html [https://perma.cc/8993-BFJZ]; *see also* Laura Smith-Spark, *Germany's Angela Merkel: Relationship with U.S. 'Severely Shaken' over Spying Claims*, CNN (Oct. 24, 2013, 1:10 PM), https://edition.cnn.com/2013/10/24/world/europe/europe-summit-nsa-surveillance/index.html [https://perma.cc/5S5M-K2PZ].

208. *See* Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291, 328–33 (2015) (describing the political pressures the U.S. faced in the aftermath of the Snowden disclosures).

209. *See, e.g.*, European Parliament Press Room, US NSA: Stop Mass Surveillance Now or Face Consequences, MEPs Say (Mar. 12, 2014), https://www.europarl.europa.eu/news/en/press-room/20140307IPR38203/us-nsa-stop-mass-surveillance-now-or-face-consequences-meps-say [https://perma.cc/SLA5-5K49].

210. *See* PPD 28, *supra* note 149.

211. *See* Benjamin Wittes, *The President's Speech and PPD-28: A Guide for the Perplexed*, LAWFARE, (Jan. 20, 2014, 11:02 AM), https://www.lawfareblog.com/presidents-speech-and-ppd-28-guide-perplexed [https://perma.cc/YK8F-QCWF] (noting that "the PPD is an exceedingly-clever document, one that conveys and writes into policy a great deal of values without constraining a great deal of practice").

212. *See* Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016, art. 45–46, 2016 O.J. (L 119) 1 [hereinafter GDPR].

213. *Id.*, art. 45(2).

214. EU Commission Decision 2000/520/EC, 2000 O.J. (L 215).

215. Case C-362/14, Schrems v. Data Prot. Comm'r (Oct. 6, 2015).

culminated in a substitute in 2016, the E.U.-U.S. Privacy Shield.[216] During the negotiations, the U.S. government "[gave] written assurances that access to [EU] citizens' personal data by the U.S. government will be subject to 'clear limitations, safeguards and oversight mechanisms,' and that any exceptions will be 'necessary and proportionate.'"[217] The Privacy Shield included a commitment from the Secretary of State to "create a new oversight mechanism for national security interference, the Privacy Shield Ombudsperson, who is independent from the Intelligence Community," and led to the passing of the Judicial Redress Act, which grants Europeans the right to file Freedom of Information Act requests.[218]

Mr. Schrems, meanwhile, petitioned again before the Irish data protection authority.[219] This time, Schrems challenged Standard Contractual Clauses (SCCs), another mechanism for data transfers. The questions raised in his complaint, along with the newly executed Privacy Shield, were referred to the CJEU for review. In *Data Protection Commissioner v. Facebook (Schrems II)*, the CJEU invalidated the Privacy Shield decision for failing to ensure privacy protections that are "essentially equivalent" to that guaranteed within the EU.[220] Although the SCCs mechanism was held lawful, the CJEU cast a long shadow over its validity by requiring data protection regulators and companies to verify on a case-by-case basis that the law of the recipient country ensures adequate protection (recall, the opinion clearly found U.S. law to be inadequate).[221] The decision puts massive pressure on U.S. and EU regulators to negotiate a new data transfer mechanism that will pass muster with the Court. In other words, the U.S. government is constrained to undertake an even more significant reform of surveillance policy than it had already done. It remains to be seen how this data transfer showdown will end, but as Europe is committed to leading on global data privacy norms, the political constraints arising from international data sharing are here to stay.[222]

---

216. EU Commission Decision 2016/1250/EC, 2016 O.J. (L 207/1) [hereinafter The Privacy Shield Decision]

217. *See* Cynthia J. Rich, *Privacy Shield v. Safe Harbor: A Different Name for an Improved Agreement?*, MORRISON & FOERSTER (Mar. 3, 2016), https://www.mofo.com/resources/insights/privacy-shield-vs-safe-harbor-a-different-name-for-an-improved-agreement.html [https://perma.cc/DEZ9-WH9J] (quoting letters provided to the EU Commission from the U.S. government).

218. The Privacy Shield Decision, *supra* note 216, at recital 65.

219. Letter by Maximilian Schrems to Ireland Data Protection Commissioner, Complaint against Facebook Ireland Ltd. (Dec. 1, 2015).

220. Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd., ¶¶ 168–202 (July 20, 2020).

221. *Id.* ¶¶ 122–49.

222. For some of the options available to the United States, *compare* Ashley Gorski et al., *The Future of U.S. Foreign Intelligence Surveillance*, JUST SECURITY (Nov. 11, 2020), https://www.justsecurity.org/73321/the-future-of-u-s-foreign-intelligence-surveillance/ [https://perma.cc/6XT5-MK2Y] (advocating comprehensive surveillance reform) *with* Stewart Baker, *How Can the U.S. Respond to Schrems II?*, LAWFARE (July 21, 2020, 8:11 AM), https://www.lawfareblog.com/how-can-us-respond-schrems-ii [https://perma.cc/N35A-M7HZ] (noting that "the time for American concessions is over").

## V. Checks and Balances in Cyberspace: Old and New

So far, I have identified and analyzed the four main parts of the cyber checks and balances ecosystem. We saw how four exogenous forces shape the digital environment, constrain the government in several ways but augment its freedom of action in others. This Part turns to normative analysis. Section A provides an assessment of the cyber checks and balances ecosystem, asking whether from a social welfarist and constitutionalist views it is beneficial or detrimental. Section B explains how this external ecosystem can be utilized to improve the traditional system of checks and balances.[223] My argument is that understanding how the external forces operate helps constitutional actors recalibrate their checking, thereby avoiding (or reducing the likelihood of) under or over constraining the Executive.

### A. A Normative Assessment

The first question to ask is what kind of work the cyber checks and balances do: are the four types of constraint described in this Article able to sufficiently mitigate the risks of government overreach? Is it possible that the aggregate impact over-constrains the Executive, giving rise to a less familiar problem, that of overly constrained executive? And, most importantly, can these forces ensure that government power is used in cyberspace for good and not for ill?

Two caveats are in order. First, it is difficult to define "good" and "ill" in this context. Cyber policy implicates many important social values. Users of cyberspace, which we all are, expect their government to provide for their security and safety on the digital sphere while upholding their privacy, personal autonomy, and liberty, and affording economic growth and innovation. The more aspects of life move to cyberspace, the more critical policy choices in this domain become. In crafting policy, decision-makers are often required to make tradeoffs between values that cannot be maximized together. Should intelligence agencies disclose or exploit vulnerabilities in technology?[224] Should regulators strictly regulate companies that handle personal data or leave this task to market forces?[225] Should technology companies be required to allow the authorities special access to encrypted communications, at the expense of users' privacy? Each choice made by policymakers inevitably advantages certain social values at the expense of others. While there are no categorical right answers to these questions, we aspire to live in a social system that encourages decision-makers to make choices that maximize the collective welfare of the

223. By "internal" I mean internal to the constitutional order. The main actors in this system are lawmakers, judges, and gatekeepers within the executive branch.

224. *See* Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, WHITE HOUSE (archived) (Apr. 28, 2014), https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities [https://perma.cc/DH6N-U6N9].

225. For the key issues at stake in the regulation of data protection, *see generally* Daniel J. Solove, *The New Vulnerability: Data Security and Personal Information* (August 9, 2011), in SECURING PRIVACY IN THE INTERNET AGE (Radin & Chander, eds., 2008), available at SSRN: https://ssrn.com/abstract=583483 [https://perma.cc/PZ9K-VQ27].

population, while vindicating the rule of law. Checks and balances play a major role in realizing this ambition.[226] As a benchmark for my analysis, I will consider any type of force or actor that pushes decision-makers along these lines of maximum collective welfare, constitutionalism, and the rule of law as normatively desirable.

Second, the principal machinery for checks and balances in democratic states is the separation of powers in government, as well as other constitutional tools such as free elections and bicameralism.[227] External checks and balances like the market, the press, and others, typically complement the internal system. These external institutions become more prominent when the constitutional separation of powers system is weak or dysfunctional.[228] This point is applicable also for present purposes: to assess the normative effect of the cyber checks and balances (which are extra-constitutional), their influence should be evaluated in relation to the internal, constitutional checks and balances.[229] The added constraints from external forces would be especially beneficial, perhaps even crucial, when the internal system does not work efficiently; but might otherwise be redundant or even harmful.[230]

With these caveats in mind, this Section considers the main advantages and limitations of the cyber checks and balances ecosystem. As will be shown, the instruments that make up this ecosystem introduce positive features into an otherwise impaired accountability regime: they help diffuse power among a greater number of actors and cast a broad net that can protect users from foreign and domestic governments. However, despite these advantages, this ecosystem is limited because it is random and unpredictable, and there is no way to ensure that its effects align with the public interest.

### B. The Diffusion of Cyber Power

The first positive consequence of the cyber checks and balances ecosystem is that it helps to diffuse power from its concentration in some constitutionally-sensitive Executive functions: law enforcement,[231] intelli-

226. For the idea that checks and balances, as part of the Separation of Powers, promote good governance, see, *e.g.*, THE FEDERALIST No. 41 (James Madison) (Clinton Rossiter ed., 1961). *See also* Huq & Michaels, *supra* note 17, at 382–88 (arguing that the separation of powers promotes "a plurality of values," including liberty, efficiency, democratic accountability, and the rule of law).

227. In the age of the administrative state, intra-executive mechanisms also serve a key role in maintaining checks and balances. *See generally* Neal K. Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 YALE L.J. 2314 (2006).

228. For an illustration, see generally GOLDSMITH, *supra* note 17.

229. *Cf.*, Deeks, *supra* note 17, at 86.

230. *Cf.*, Abebe, *supra* note 178, at 125.

231. *See, e.g.*, Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y. U. L. REV. 1827 (2015) (arguing that "laws governing the police are notably sparse—if they exist at all" and that the democratic accountability of policing agencies is limited and suboptimal).

gence collection,[232] national security,[233] and foreign affairs.[234] In these areas, the Executive typically exerts great influence over decision-making because it controls the information and is less constrained by law.[235] The concentration of power in the Executive is a tenacious phenomenon that over time erodes democratic accountability of decision-makers and adherence to the rule of law.[236]

Against this backdrop, cyber checks and balances play an important constitutional role by helping to diffuse power along three important axes: (1) power in international relations; (2) power between government and private actors; and (3) control of information.[237]

*Power diffusion in international relations.* In the physical domain, chief executives of militarily powerful nations have grown accustomed to making major national security decisions unilaterally, rarely being challenged ex-ante or forced to face significant consequences for bad or illegal decisions ex-post. President Obama authorized targeted killings of suspected terrorists in numerous theaters of operation without clear legal authorization from Congress.[238] Prime Minister Tony Blair committed Britain to the Iraq war on a false pretense that the war was necessary to disarm Iraq's WMD

232. *See, e.g.*, Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1 (2008) (describing the oversight deficit with respect to the "national surveillance state").

233. *See, e.g.*, HAROLD H. KOH, THE NATIONAL SECURITY CONSTITUTION (1990) (describing how Congress and the courts have failed to check presidential war powers); CHARLIE SAVAGE, TAKEOVER: THE RETURN OF THE IMPERIAL PRESIDENCY AND THE SUBVERSION OF AMERICAN DEMOCRACY (2007) (arguing that the War on Terror enabled the presidency to undermine the constitutional system of checks and balances).

234. *See* Curtis A. Bradley, *A New American Foreign Affairs Law?* 70 U. COLO. L. REV. 1089, 1096 (1999) (arguing that "the federal government's foreign affairs powers are subject to a different, and generally more relaxed, set of constitutional restraints than those that govern its domestic powers").

235. *See generally* ERIC A. POSNER & ADRIAN VERMEULE, THE EXECUTIVE UNBOUND: AFTER THE MADISONIAN REPUBLIC (2010) (analyzing the failure of law and the separation of powers to constrain presidential power, specifically in the areas of war making, foreign policy, and emergencies); Robert D. Sloane, *The Scope of Executive Power in the Twenty-First Century: An Introduction*, 88 B.U. L. REV. 341 (2008) (describing the evolution of theories rationalizing executive unilateralism); ARTHUR M. SCHLESINGER, JR., THE IMPERIAL PRESIDENCY (2004) (describing the gradual expansion of presidential power, especially over war-making and foreign affairs). For accounts outside the U.S. context, see MARGIT COHN, A THEORY OF THE EXECUTIVE BRANCH TENSION AND LEGALITY (2021); DAVID DYZENHAUS, THE CONSTITUTION OF LAW 42–47 (2006) (discussing executive dominance in national security decision-making in the Commonwealth countries).

236. The repercussions of executive monopoly over power to citizens might even be more dangerous in cyberspace, as the collateral harm to the rights of citizens appears greater in the digital space than in kinetic domains where security activity is often projected extra-territoriality and targeted at foreigners.

237. To be sure, the diffusion of powers imposes costs as well, in the sense that adversaries may be better able to act harmfully to public and private interests.

238. *See* WHITE HOUSE, REPORT ON THE LEGAL AND POLICY FRAMEWORKS GUIDING THE UNITED STATES' USE OF MILITARY FORCE AND RELATED NATIONAL SECURITY OPERATIONS (2016).

program.[239] Israel's PM Netanyahu has authorized recurring air strikes against Iranian proxy targets in Syria, with little regard to Syria's sovereignty.[240] Lastly, President Trump ordered the killing of Iranian General Qasem Soleimani, relying on questionable legal justifications.[241] These executives were able to act because of their nations' military superiority and because it was difficult for anyone outside their administration to check the facts or challenge the legal rationale for their decisions.

The diffusion of cyber power among many state and non-state actors makes this sort of behavior harder.[242] In cyber, the power gaps are narrower and states like the United States, Britain, and Israel are more vulnerable to retaliation.[243] Israel does not dominate the cyber sphere on the same level as it dominates Syria's airspace;[244] and the United States did not respond harshly to Iranian attacks on the financial sector, the Sony hack, and Russian election meddling, because it knew that a cycle of escalation would inflict more damage on American networks than was tolerable.[245] This is not to argue that Russian and Iranian hackers play a positive role in the American system of checks and balances, but the diffusion of cyber power does create an effect similar to that created by checks and balances: imposing constraints on the ability and will of the government to take certain action, and in this case, use force. Given that there are arguably insufficient incentives for executives to avoid the unnecessary use of force in the physical domain, especially in the age of drones and remote warfare, these pressures may have some benefits in cyberspace.[246]

---

239. *Chilcot Report: Key Points from the Iraq Inquiry*, THE GUARDIAN (Jul. 6, 2016), https://www.theguardian.com/uk-news/2016/jul/06/iraq-inquiry-key-points-from-the-chilcot-report [https://perma.cc/LJ7P-5NWG].

240. *See* Amichai Cohen & Elena Chachko, *The Israel-Iran-Syria Clash and the Law on Use of Force*, LAWFARE (Feb. 14, 2018, 10:47 AM), https://www.lawfareblog.com/israel-iran-syria-clash-and-law-use-force [https://perma.cc/DHV5-C4US].

241. *See generally* CONTEXT AND CONSEQUENCES OF THE SOLEIMANI STRIKE, LAWFARE INST. (E-Book) (2020).

242. *See* Nye, *supra* note 180 (describing the reasons and implications of cyber power diffusion among states); *see also* Eichensehr, *Digital Switzerlands*, *supra* note 12, at 712–15 (describing the shift of certain powers to multinational tech companies).

243. *See* Nye, *supra* note 180, at 9 ("The diffusion of power in the cyber domain is represented by the vast number of actors, and relative reduction of power differentials among them"); Goldsmith & Russel, *supra* note 16, at 1–2 (arguing that the strengths of American society create asymmetrical vulnerabilities in the digital age that foreign adversaries, especially in authoritarian states, are increasingly exploiting).

244. *See* Catalin Cimpanu, R*ecent Ransomware Wave Targeting Israel Linked to Iranian Threat Actors*, ZDNET (Nov. 11, 2020, 6:32 PM), https://www.zdnet.com/article/recent-ransomware-wave-targeting-israel-linked-to-iranian-threat-actors/ [https://perma.cc/CQ5Y-2QTZ] (reporting a wave of cyber-attacks linked to Iranian sources that targeted Israeli companies).

245. *Id.* at 8 ("it appears that the fear of losing in escalation due to asymmetrical digital dependence is one of the main reasons why the US government has hesitated to retaliate in recent years in the face of increasingly damaging cyber operations from abroad").

246. Indeed, the modern war powers debate has evolved around instances of presidential uses of force that in hindsight seemed unnecessary and unconstitutional, and Congressional effort to respond by creating stronger constraints on the President. *See*

*Power diffusion between government and private actors.* A similar dynamic is at play between states and private companies. As discussed in Part IV, the private sector exerts various forms of soft and hard power in cyberspace: companies develop privacy-enhancing technologies, advocate international norms and accountability mechanisms, and offer surveillance and offensive cyber services for hire. The rise of corporate cyber power represents a decline in governmental cyber power, as it provides corporate actors with the ability to disrupt or otherwise impose costs on governmental cyber activities that are at odds with their own interests. Earlier, we saw how internet intermediaries were able to challenge U.S. surveillance policy.[247] Consider two more recent examples. First, in 2020, in the wake of several incidents of police brutality across the United States, Microsoft joined Amazon and IBM to announce that it would not sell face-recognition technology to the police "until we have a national law in place, grounded in human rights, that will govern this technology."[248] The companies capitalized on their control of the technology to raise awareness to what they believed was an illegal police practice and made it harder for the government to acquire the products enabling that practice. Second, in the context of the coronavirus pandemic, Apple and Google—who jointly control 99.6 percent of the mobile operating systems (OS) market[249]—were able to halt digital contract tracing systems of several countries in Europe for failing to meet their OS privacy demands.[250] As the fight against the spread of Covid-19 required societies all over the world to strike a balance between health and privacy, many countries faced a dire dilemma: accept Apple and Google's dictates, or run a sub-optimal contact tracing app.[251] This dilemma has obvious constitutional implications, for it means that the tradeoff between fundamental values and public policy goals is made not only by legally-established public institutions, but also by technology companies. As these examples make clear, power diffusion between govern-

*generally*, DAVID J. BARRON, WAGING WAR: THE CLASH BETWEEN PRESIDENTS AND CONGRESS, 1776 to ISIS (2016).

247. *See supra*, notes 41–52 and accompanying text.

248. Jay Greene, *Microsoft Won't Sell Police its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM*, WASH. POST (June 11, 2020, 9:30 PM) (quoting Microsoft president Brad Smith), https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/ [https://perma.cc/D8YV-JAXC].

249. *See* Mobile Operating Systems' Market Share Worldwide From January 2012 to January 2021, Statista (Feb. 8, 2021), https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/ [https://perma.cc/CGZ2-PHEM].

250. *See* Iana Ilves, *Why are Google and Apple Dictating How European Democracies Fight Coronavirus?*, GUARDIAN (June 16, 2020, 4:00 PM), https://www.theguardian.com/commentisfree/2020/jun/16/google-apple-dictating-european-democracies-coronavirus [https://perma.cc/R9G5-Y77G].

251. Some states, like the U.K. and Germany, ultimately decided to accept Apple and Google's demands and adopt their decentralized notification technology, while France insisted moving forward with its original system after admitting that it would not function optimally on Apple and Google devices. *See* Mark Scott et al., *How Google and Apple Outflanked Governments in the Race to Build Coronavirus Apps*, POLITICO (May 15, 2020, 5:25 AM), https://www.politico.eu/article/google-apple-coronavirus-app-privacy-uk-france-germany/ [https://perma.cc/L4SN-ECL7].

ment and private actors might have both social costs and benefits, but it at least serves a separation of powers function in areas traditionally controlled by the Executive.

*Control of information.* The fact that private actors control or operate many parts of the physical and virtual properties of cyberspace means that in many situations these actors "[bring] to the table irreplaceable access to information and infrastructure that the Executive needs to perform its job."[252] This is yet another aspect in which diffusion of power helps create better conditions, which have the effect of checking the Executive in the cyber domain. In the physical domain, the Executive has better and often exclusive access to information relating to certain areas such as national security and foreign affairs, which it frequently is reluctant to share with outside actors.[253] The control of information has benefits and costs: it allows executives to minimize leaks endangering security and intelligence efforts on the one hand, but limits oversight and covers up incompetence and corruption in the Executive, while also encouraging biased decision-making on the other.[254] Information control is also prone to abuse, creating different problems ranging from excessive secrecy or "overclassification" to lies and fabrication of facts.[255]

But information obtained, produced, or disseminated in cyberspace is less susceptible to these pathologies, mainly because of the ways that companies interact with it. To increase the nation's cyber resilience, governments willingly share classified information with technology and companies involved with critical infrastructure.[256] In other cases, when governments seek to obtain the emails of suspected terrorists or discover new software vulnerabilities, they rely on cooperation with the private sector, which requires some level of information sharing. In still other cases, companies find alternative paths to obtain sensitive information that governments would prefer to conceal from the public eye.[257] The roles of

252. Deeks, *Secrecy Surrogates*, *supra* note 17, at *6.

253. *See* Cass R. Sunstein, *The Most Knowledgeable Branch*, 164 U. PA. L. REV. 1607 (2016) (analyzing the sources of the executive's informational advantage and its implications); *see also* Josh Chafetz, *Whose Secrets?*, 127 HARV. L. REV. FORUM 86, 87 (2013) (criticizing the common tendency to treat government secrets as a property of the executive branch and noting that "executive branch officials determine what information is secret, a determination to which other political actors are expected to (and do) defer").

254. For the arguments for and against state secrecy, *see generally* David Pozen, *Deep Secrecy*, 62 STAN. L. REV. 257, 275–92 (2010); Deeks, *Secrecy Surrogates*, *supra* note 17, at *9–12.

255. *See* Elizabeth Goitein & J. W. Leonard, *America's Unnecessary Secrets*, N.Y. TIMES (Nov. 7, 2011), https://www.nytimes.com/2011/11/07/opinion/national-security-and-americas-unnecessary-secrets.html?auth=login-google [https://perma.cc/8YCN-7Q8B] (considering the harms resulting from overclassification); *see also* Shalev Roisman, *Presidential Factfinding*, 72 VAND. L. REV. 825, 871–72 (2019) (surveying examples of lies told by U.S. presidents over information under their control).

256. In an era when many national critical services are privatized, the practice of threat information sharing is becoming vital for assessing and mitigating risks. *See* SOLARIUM COMM'N REP., *supra* note 56, at 55–56. This increases the number of actors with access to information otherwise held exclusively by the Executive.

257. Private attribution of cyber-attacks is a paradigm of this category. *See supra* notes 57–64 and accompanying text.

companies as consumers, intermediaries, and vendors of sensitive information provide them with a glimpse and, sometimes, a hard look at how governments obtain, treat, and use information. With this power, they are able to challenge the traditional monopoly of the Executive on information relating to security and foreign affairs. As scholars have shown, it often appears that the companies also believe it is in their interest to do so.[258]

### C. Extraterritorial Effects

Another important feature of cyber checks and balances is their extraterritorial effect. Constitutions constrain domestically: they are meant to set limits on how our governments govern us. But in a domain in which foreign actors can steal, destroy, and distort our data, it is critical to have a system that can directly restrain such actors as well as. A law banning digital surveillance enacted in Sweden does not have any real constraining power on Russian hackers who seek to collect the personal data of Swedish citizens, but strong encryption does: its constraining effect surpasses the territorial limitations of constitutional checks and balances.

Should this feature be counted as a virtue or a vice? It is probably a little of both. It is an advantage in the sense that it closes a regulatory gap between the government of one country and individuals of other countries that may be directly affected by cyber activities carried out by that government. Gone are the days when international relations concerned only governments. Today, individual privacy and data security are threatened daily by foreign governments and other non-state foreign actors; and everyone has a stake in internet security. Cyberattacks such as NotPetya and the data breaches such as the Equifax hack, both carried by foreign governments but affected individuals, provide examples. They demonstrate why individuals have a legitimate interest in constraining the ability of foreign governments and other foreign actors to harm them. Constitutional checks and balances fall short of that goal, but cyber checks and balances are effective tools and thus desirable.

However, the influence of external forces on government behavior is also a vice, as it runs contrary to the principle of democratic governance.[259] Is it in our national interest to have non-democratic forces and actors shaping our government's actions in cyberspace? Arguably, if the voices of foreign actors, e.g., international institutions, foreign governments, and private companies, are amplified, then the voices of citizens and democratic institutions are diminished. In the Apple and Google example discussed above, one line of criticism may argue that private foreign companies should not dictate the appropriate balance between health and privacy of sovereign nations. This decision should be made by the citizens of each country through their democratic institutions.

---

258. *See, e.g.*, Eichensehr, *Digital Switzerlands*, *supra* note 12, at 714.

259. Abner S. Greene, *Checks and Balances in an Era of Presidential Lawmaking*, 61 U. CHI. L. REV. 123, 132 (1994) ("Diversifying the voices heard in government not only helps to prevent one point of view from becoming too strong, but also promotes the affirmative goal of democratizing governmental decisionmaking.").

This sort of criticism, which alludes to a lack of democratic legitimacy, is familiar in debates over international law and can readily be extended to the present discussion.[260] The objection is that international law is not made by representatives elected by and accountable to the citizens, and that the process through which it is created is less visible to public scrutiny than domestic lawmaking.[261] Its normative domestic impact thus weakens the connection between the governed and the rules governing them, undermining the legitimacy of the latter. This critique, with some adaptation, can be leveled against each of the four constraints discussed in this Article: although they simulate what checks and balances do, the actors behind them—foreign governments and companies—are not domestically accountable. These actors usually seek to promote interests that the local public is either agnostic about (e.g., raising their share value, in the case of companies) or objects to (e.g., the interests of adversarial governments).[262]

So, we can see that the extraterritorial nature of cyber checks and balances is both a virtue and a vice. In assessing the net effect, it is important to bear in mind that for many of the areas discussed in this Article, including national security and law enforcement, decision-makers are not sufficiently democratically accountable. In these circumstances, even constraints that originate from non-democratic forces can be accountability enhancing. They encourage more caution among decision-makers, who are more visible to scrutiny, bring valuable information to the public, and elicit more energetic engagement by courts and legislatures.[263]

These rationales apply with some force to the cyber context—the Executive has informational advantage (though, not monopoly on information) and more democratic accountability compared to other relevant actors—although the analogy is not perfect. The cost-imposition theory is useful because it helps frame the questions on the role of external checks: can we trust an external checking ecosystem that, through four types of constraints, raises the costs of governmental cyber activities that may infringe on individual rights? Are these constraints robust enough to filter out "bad" cyber policies but allow "good" policies to move forward? Arguably, if they come close to it, this may suggest that the Executive is sufficiently "regulated" and that we need to rely less on the traditional checks—law and the political process. If not, tighter legal and democratic control of the

260. *See, e.g.*, McGinnis & Somin, *supra* note 135, at 1193–95; Mattias Kumm, *The Legitimacy of International Law: A Constitutionalist Framework of Analysis*, 15 EU. J. INT'L. L., 907, 907–09 (2004); Ernest A. Young, *The Trouble with Global Constitutionalism*, 38 TEX. INT'L. L. J. 527 (2003).

261. McGinnis & Somin, *supra* note 135, at 1193–97.

262. *Cf*., Deeks, *supra* note 17, at 88 (arguing, in the context of intelligence oversight by foreign allies, that "the reasons and values behind the external checks . . . may not be values that the US demos would support").

263. *See* Rozenshtein, *supra* note 12, at 176 ("by empowering actors within the government that can check executive branch surveillance—whether the other branches of government or intra-executive actors—surveillance intermediaries help ensure that a wider (and thus more representative) cross-section of the government generates surveillance policy").

Executive's cyber policies might be justified. Either way, under this theory, the external checks have a holistic positive influence.

### D. Unpredictable Effects

Although the lack of democratic accountability is a significant limitation of the cyber checks and balances ecosystem, I think that its principal flaw lies in its unpredictable nature. This ecosystem's four constituent parts constrain government power based on different incentive structures, aiming to serve goals that are largely detached from popular sentiment. The overall level of constraint they produce is hard to predict; their motivation and ideologies vary, and it is impossible to ensure the durability and intensity of their checking.

Consider two examples. First, attribution of cyberattacks. "Figuring out who's doing what to whom and publicly identifying those responsible for bad acts in cyberspace are key elements of increasing efforts to hold those actors more accountable."[264] Private actors have a central role in performing this important function. As scholars have shown, private attribution of state-sponsored cyber-attacks occurs when firms are sufficiently motivated and technically capable of collecting and analyzing the digital evidence of an incident. Yet neither factor is present for every incident, and as a result, checking from private attribution occurs sporadically, often affected by national and political considerations. Another example is the going dark issue. Despite all of the fuss about law enforcement agencies loss of access to digital evidence and its impact on security-privacy debates, encryption actually restricts government access to information at an unknown rate. Not all companies encrypt their products and services; those who do may choose to keep a copy of the exchange key, a choice that may give governments special access to encrypted data. Moreover, not all data can be encrypted (metadata for example). And finally, the capacity to break encryption varies across governments and across agencies. In most cases, people outside the government lack information of what types of cryptographic systems actually block government access.

Moreover, in a well-functioning system of checks and balances, it is expected that different checks are synced and react to one another. Courts check the Executive more assertively when the political process fails,[265] and they tend to be more deferential when the two other branches act in concert.[266] Here, however, the different parts of the "system" usually act independently and randomly. The architecture of the internet—the ways data are routed and secured—has little to do with the extent to which international law places limits on state behavior. Private firms do not decide when and how much to oppose governments in cyberspace based on international politics; they make these decisions as part of a strategy for maximizing profits for their shareholders (although, this may entail giving some

264. Eichensehr, *Cyberattack Attribution*, *supra* note 60, at 522.
265. *See, e.g.*, United States v. Carolene Prods. Co., 304 U.S. 144, 152 n.4 (1938).
266. *See, e.g.*, Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952).

weight to geopolitical considerations).[267] When every feature of a checks and balances system acts independently, it is more likely to have cases of over and under-constraint.

Another problem is that to appreciate the overall level of constraint produced by this system, one must also consider the various ways through which it enhances executive power, and then offset the power-enhancing effects from the constraining effects. A good illustration is the perceived role of internet companies in government surveillance: for some, the tech industry's growing tendency to use end-to-end encryption is what causes the "going dark" problem; for others, the "golden age (of surveillance)" terminology is more appropriate to describe what the industry is really responsible for. Both views are correct: internet intermediaries constrain, that is, raise the costs of surveillance in certain ways, but also make it more possible by virtue of their own massive surveillance practices. In order to examine the efficacy of "surveillance intermediaries" as a check, we need to measure and compare both effects, which are indeterminate and normatively contested.[268]

### E. Constitutional Checks and Cyber Checks

As both the importance of the internet to social existence and the dangers emanating from cyberspace continue to expand, it may be expected that governments will regulate cyberspace even more than they do today. The seeds for additional regulation have already been sown. Incidents like the SolarWinds intrusion,[269] in which foreign actors were able, through a supply-chain attack against a private software company, to penetrate sensitive government and private networks, may justify aggressive government action, not only as a regulator but also as an active operator in private networks.[270] Efforts to manipulate users of social media and spread disinformation, seen during the coronavirus pandemic, may set the stage for proposals to curb online speech. As observed by Jack Goldsmith and Andrew Woods, "the trend toward greater surveillance and speech control

267. Occasionally, external checks do act reactively to one another. For example, private initiatives to promote global norms of state behavior in cyberspace can be viewed as a response to the failure of the GGE process and subsequent split between the Western-led and Russian-led efforts to clarify how international law applies to cyberspace.

268. *See* Alan Z. Rozenshtein, *Wicked Crypto*, 9 U.C. IRVINE L. REV 1181, 1200–06 (2019) (explaining why creating consensus on the desired level of surveillance is difficult).

269. *See* FIREEYE, *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor* (Dec. 13, 2020), https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html [https://perma.cc/28JT-P3ZN].

270. *Cf.* Cyber Security and National Cyber Directorate Bill 2018 [Isr.] (authorizing the Israeli Cyber Directorate, subject to a judicial warrant, to perform cybersecurity actions in computers of private companies covered under the Bill). For analysis of the Bill in English, see Amir Cahane, *The New Israeli Cyber Draft Bill - A Preliminary Overview*, CYBERLAW BLOGSPACE - THE FEDERMANN CYBER SECURITY RESEARCH CENTER – CYBER LAW PROGRAM (2019), https://csrcl.huji.ac.il/news/new-israeli-cyber-law-draft-bill [https://perma.cc/439L-PGY2].

[. . .], and toward the growing involvement of government, is undeniable and likely inexorable."[271] These recent developments raise the stakes for reaching an appropriate balance between power and its constraint in cyberspace. Cybersecurity measures aimed to make cyberspace safe and free from manipulation can easily spill over to actions that disproportionally compromise civil rights, including unchecked surveillance, censorship, and limitations on privacy in violation of due process.[272] Keeping such measures in check is a major challenge for constitutionalism and the rule of law in our time.

The foregoing analysis provides little basis for hope that external constraints will be able to form an efficient checks and balances mechanism that would perhaps excuse inaction by the actors officially entrusted with this role. Understanding how the cyber ecosystem works in practice affords those same actors an opportunity to better calibrate their checking and balancing role.[273] Taking account of the diverse constraints that shape cyber policy would afford lawmakers, judges, and intra-executive actors the occasion to redirect their efforts and resources more effectively.

Here are two examples. First, let's revisit the issue of vulnerabilities disclosure—the dilemma governments face when they decide whether to disclose or exploit security flaws in technology. This is a genuinely difficult problem for cybersecurity: the decision often entails predictions about uncertain risks (will hackers or adversarial governments discover this vulnerability?), as well as a choice between variants of "security" as a social value (should we favor general security for users of cyberspace over the ability to collect better intelligence and hack adversaries' networks?). The question is how to ensure that the so-called "vulnerabilities equities process" (VEP), which is carried on by executive officials with a bias toward exploiting vulnerabilities,[274] will be based on objective and careful consideration of the costs and benefits and include sufficient safeguards against loss of data, abuse, and mismanagement of maintained vulnerabilities.[275] Currently, this issue avoids regulation and oversight by constitutional mechanisms. Instead, it is subject to an interagency process within the executive branch, a sort of self-checking mechanism with little to no

271. Goldsmith & Woods, *supra* note 9.

272. *See* National Res. Council, At the Nexus of Cybersecurity and Public Policy, 100–03 (David Clark et al eds., 2014).

273. Daniel Abebe introduced a similar argument in considering the relationship between international politics and the President's constitutional war authority in cyberspace. His logic fits well regarding the broader cyber checks and balances ecosystem. *See* Abebe, *supra* note 200, at 2.

274. Officials in law enforcement, intelligence and national security agencies are judged first and foremost by their success in prosecuting crimes, collecting intelligence, and countering national security threats. As a result, the average official is prone to "pay less heed" to the costs of zealousness in pursuing these goals. *Cf*., Rascoff, *supra* note 18, at n.285.

275. For analysis of proposals for reform, *see* Sven Herpig & Ari Schwartz, *The Future of Vulnerabilities Equities Processes Around the World*, LAWFARE (Jan. 4, 2019, 12:30 PM), https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world [https://perma.cc/WF8E-LTEU].

transparency.[276]

Is this accountability regime appropriate? Taking account of the overall level of constraints imposed by the external cyber ecosystem provides valuable insights to answer the question. This example may suggest that the current regime is inadequate. For starters, the Executive faces minimal, if any, external constraints. VEP decisions are not regulated under international law.[277] There are no political pressures by other nations or nonstate actors that may affect VEP decisions and act as a counterweight to a pro-national security bias, i.e., contra surveillance policy. And no forces from architecture or the private sector have any constraining effect against amassing vulnerabilities for national security purposes. Furthermore, some forces within this ecosystem even augment executive power, by enabling the executive to circumvent the VEP, which, in the current regime, is the only check against mishandling of software vulnerabilities. The development of a vibrant market of hacking services, companies that discover or purchase vulnerabilities, weaponize them, and offer their hacking tools to governments, creates a loophole. Governments may hire such companies to de-facto exploit vulnerabilities without submitting to VEP review if they do not purchase "the rights to the technical details from the third-party seller."[278] This is exactly what the FBI did when it hired a private company to crack a locked iPhone used in a terrorist attack in San Bernardino, California.[279]

Inadequate constraints on the Executive from the cyber ecosystem and the fact that external actors enhance government ability to bypass the only accountability mechanism in place are telling. Internal processes, like the VEP review, have limited constraining force without additional checking by the courts and the legislature.[280] When the influence of external actors, who help create additional loopholes in this fragile accountability mechanism is added, the result is an inadequate accountability regime. Absent

276. *See* Vulnerabilities Equities Policy and Process for the United States Government, November 15, 2017. For the U.K. VEP, see Government Communications Headquarters, The Equities Process (Nov. 29, 2020), https://www.gchq.gov.uk/information/equities-process [https://perma.cc/89ZE-XJLA]. Other countries, such as the Netherlands, Germany, and Australia have crafted or are developing VEP processes along similar lines.

277. *See* Kate Charlet et al., *It's Time for the International Community to Get Serious about Vulnerability Equities*, LAWFARE (Nov. 15, 2017, 1:00 PM), https://www.lawfareblog.com/its-time-international-community-get-serious-about-vulnerability-equities [https://perma.cc/TEE2-TGT8] (urging the international community to begin a conversation about the international legal dimensions of vulnerability management).

278. Mimansa Ambastha, *Taking a Hard Look at the Vulnerabilities Equities Process and its National Security Implications*, BERK. TECH. L.J. BLOG (Apr. 22, 2019), https://btlj.org/2019/04/taking-a-hard-look-at-the-vulnerable-equities-process-in-national-security/#_ftn49 [https://perma.cc/WRT9-9FFH].

279. Don Resinger, FBI: Sorry, But We're Keeping the iPhone Crack Secret, FORTUNE (Apr. 27, 2016, 8:06 PM), https://fortune.com/2016/04/27/fbi-apple-iphone-crack/ [https://perma.cc/YJ5D-9WTP].

280. *See, e.g.*, David Pozen, *Privacy-Privacy Tradeoffs*, 83 U. CHI. L. REV. 221, 244 (2016) (cautioning against executive autonomy in the regulation of risk-risk tradeoffs; noting that "because each has its own interests, culture, and constituency, any given institution is liable to discount or overlook at least one side of any given tradeoff").

sufficient external checking, courts and legislatures should rethink their passivity on the issue. Without attempting full resolution of the problem, which is beyond the scope of this Article, a law governing the process may be necessary. Such a law may grant limited authority to exploit software flaws and withhold them from vendors under certain conditions and, subject to proper safeguards, including reporting obligations and some form of judicial review.

A second example, mentioned earlier in passing, is the issue of contact tracing apps. In early 2020, as SARS-CoV-2 began to spread across the world, many governments turned to data-driven technologies for answers. Contact tracing was one important area in which it was believed that technology could make a critical contribution.[281] Governments, research institutions, and for-profit corporations—headed by Apple and Google, led, participated, funded, and collaborated in efforts to automate contact tracing. Deploying apps that essentially keep a log of contacts or movements obviously raises serious human rights concerns and anxieties reminiscent of an Orwellian surveillance state.[282] What is the optimal balance between power and constraint, in the face of such a dire risk to public health on the one hand and human rights on the other? How should legislatures and courts respond to policy initiatives seeking to use digital contact tracing tools to control the spread of the disease?

This problem, I suggest, needs to be approached with awareness of the external cyber ecosystem. In this case, the constraints imposed by external forces were significant and required more subtle checking and balancing within the system. In Europe, regional legal institutions like the EU Data Protection Board demanded member states adhere to strict privacy rules in designing and using contact tracing apps.[283] Along with other EU bodies and national data protection bodies, the EU Data Protection Board created legal-political settings in which governments were forced to limit the efficacy of their preferred apps to meet privacy and data protection restrictions.[284] Even more imposing were the constraints from architecture and the private sector. As noted, Apple and Google were able to leverage their

281. *See generally* Hannah Murphy, *US and Europe Race to Develop 'Contact Tracing' Apps*, FINANCIAL TIMES (Apr. 3, 2020), https://www.ft.com/content/d42acff2-b0b5-400b-b38f-ec621d4efd95 [https://perma.cc/3BA4-5TVD].

282. *See, e.g.*, Justine Pila, *Covid-19 and Contact Tracing: A Study in Regulation by Technology*, 11 EU. J. L. TECH. (forthcoming, 2021), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3749504 [https://perma.cc/7FX8-3Z2M] (discussing the risks to human rights and democratic values created by the use of disease surveillance apps).

283. *See* EU Data Protection Board, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (Apr. 21, 2020).

284. The Norwegian app, which traced movements and recorded locations on a centralized server provides an example. In August, the EU and Norwegian Data Protection Authority banned the app, overruling the position of the country's Institute of Public Health, after it was found to impose disproportionate "intervention in the users' fundamental rights to data protection." EU Data Protection Board, Temporary Suspension of the Norwegian Covid-19 Contact Tracing App, EUDPB National News (June 22, 2020), https://edpb.europa.eu/news/national-news/2020/temporary-suspension-norwegian-covid-19-contact-tracing-app_en [https://perma.cc/H3EC-ZQZA].

monopoly over smartphone operating systems to dictate the rules governing contact tracing.[285]

The Google-Apple application programming interface (API) overcame a major technological obstacle for customized apps that rely on Bluetooth technology. Particularly on Apple devices, apps running in the background were not allowed to access Bluetooth and obtain new contacts. To perform this essential function, the user was required to keep the phone unlocked with the app running in the foreground at a cost in battery life and convenience. The new API resolved the issue but enforced strict rules. Apps designed for the new interface are not allowed to collect location data; their communication protocol must be decentralized; they must receive user consent for operating and separate consent for sharing the data with public health authorities; and data collected are subject to strict minimization rules.[286] In other words, governments that sought to use the more advanced Bluetooth technology had to play by the rules set by the two tech giants.[287] Some countries, like the U.K., Norway, and Germany, ultimately decided to accept Apple and Google's dictates and abandoned the tracing models they initially found most useful.[288] Especially in the U.K., the shift caused major setbacks in the launch of new apps.[289] Other countries, including France, Israel, Australia, and New Zealand, insisted on moving forward with their original systems, admitting that they would not function optimally on Apple and Google devices. France and Germany asked Apple to relax some of the iPhone privacy features that diminish the functionality of their desired apps, but the company did not bend.[290]

In the face of these constraints, the very ideas that checks and balances were meant to prioritize safeguarding democratic governance were compromised. It made little sense for lawmakers to impose more constraints on the Executive, but this was exactly what some of them did.[291] A wiser response would have been first to address the issue at hand, or, as Alan Rozenshtein described it, "combat the technological unilateralism"

---

285. *See* Scott, *supra* note 251.

286. *See* Patrick Howell O'Neill, *Google and Apple Ban Location Tracking in Their Contact Tracing Apps*, MIT TECH. REV. (May 4, 2020), https://www.technologyreview.com/2020/05/04/1001060/google-and-apple-lay-out-rules-for-contact-tracing-apps/ [https://perma.cc/AD6E-Q5HZ].

287. *See* Scott et al., *supra* note 251.

288. *See* Sam Shead, *In Major U-turn, the UK will Now Use Apple and Google's Platform for its Coronavirus Tracing App*, CNBC (June 18, 2020, 1:02 PM), https://www.cnbc.com/2020/06/18/apple-and-googles-tech-to-underpin-uk-contact-tracing-app.html [https://perma.cc/9FKU-KLJY].

289. *See* Rory Cellan-Jones, *Coronavirus: What Went Wrong with the UK's Contact Tracing App?*, BBC NEWS (June 20, 2020), https://www.bbc.com/news/technology-53114251 [https://perma.cc/9V5T-ZNZR].

290. *See* Scott et al., *supra* note 251.

291. For example, lawmakers in South Carolina blocked state agencies from implementing contact tracing apps using the Apple and Google platform. *See* Dave Perera, *South Carolina Legislature Puts Coronavirus Apps on Hold*, M.LEX (June 26, 2020, 5:00 PM), https://mlexmarketinsight.com/insights-center/editors-picks/area-of-expertise/data-privacy-and-security/south-carolina-legislature-puts-coronavirus-apps-on-hold [https://perma.cc/LZZ7-QNAN].

imposed by the companies.[292] Lawmakers could then regulate, by creating a legal framework to allow the Executive some flexibility in choosing its preferred technology, while, at the same time, placing appropriate safeguards to minimize the risks. Given the dire outcomes of the COVID-19 crisis around the world, I doubt that the biggest problem was too much surveillance.[293] The lesson to be learned is that considering the external forces at play would have enabled a more informed legal response to the pandemic.

**Conclusion**

This Article is about balance between power and constraint in cyberspace. As more aspects of our lives move to the digital domain, and more rogue actors, states and non-states, seek to take advantage of our increasing dependency on technology, this question becomes critical. People need government powerful enough to protect against novel threats and capable enough to harness technology, but not too powerful to encroach disproportionately on individual rights, such as privacy, liberty, and speech. Aspects of this challenge have been addressed before by scholars, but the forces and actors that shape government behavior are diverse, and the interrelationship between them is complex. In laying out relevant factors and considering their dynamics with the forces within the system of constitutional checks and balances, this Article takes the first steps in studying ways to improve democratic accountability in cyberspace.

---

292. Rozenshtein, *supra* note 12, at 181.

293. As of this writing, on January 19, 2021, there are more than 93 million confirmed cases, including 2.03 million deaths globally. Over 500,000 new cases were confirmed yesterday; and many countries are in the midst of a second wave or the beginning of what appears to be a third wave of the outbreak. See WHO Coronavirus Disease (COVID-19) Dashboard (Data last updated: Feb. 3, 2021, 9:45AM CET), https://covid19.who.int/?gclid=CJwKCAiArIH_BRB2EiwALfbH1Kc9eEMk_-nO7P1xjsL0ceB8Gl29RQh7pL24L_ZJfOdMTeTCQtLkVhoCFIwQAvD_BwE [https://perma.cc/S5M5-K4EV].