THE USER, THE SUPERUSER, AND THE REGULATOR: FUNCTIONAL SEPARATION OF POWERS AND THE PLURALITY OF THE STATE IN CYBER

Eldar Haber[†] *& Amnon Reichman*[††]

ABSTRACT

Beyond a shared understanding that regulating cyber is complex, the role the state plays in this domain has thus far eluded systemic analysis. This Article addresses this gap by offering a working definition of "cyber" and proceeds unearthing the polycentric roles and functions performed by various state organs in relation to digital-to-digital defense, offense, and surveillance. More specifically, the Article details the institutional matrix within which the state operates in cyber, and then sheds an innovative light on the potential tensions between the state in its capacity as a user, a "superuser," and a regulator. As users of networked products and services, public entities depend on the developers and providers of such products and services, just like any other user. As a superuser, the state belongs to an exclusive club of a handful of entities that have the capacity to act in cyber in a manner that affects many, if not all, other players by engaging in offense, defense, and surveillance on a large scale and at high intensity. The regulatory capacity of the state is not only dispersed among multitude of agencies and faces challenges by the domestic and transnational industry, but is also confronted with the conflicting demands of users (including public users), seeking protection and a stable environment for innovation, and superusers (including state-run superusers), seeking exemptions in return for cooperation with the regulatory agenda and a commitment to maintain a qualitative edge vis-à-vis adversaries. The Article concludes by offering a preliminary set of recommendations designed to address these tensions.

DOI: https://doi.org/10.15779/Z38V40K05C

† Senior Lecturer, Faculty of Law, University of Haifa; Faculty member, Center for Cyber, Law and Policy (CCLP), and Haifa Center for Law and Technology (HCLT), University of Haifa.

†† Robbins Collection Visiting Professor of Law, UC Berkeley; Professor of Law, University of Haifa; Director, The Center for Cyber, Law and Policy, University of Haifa, Principal Investigator, The Minerva Center for the Study of the Rule of Law Under Extreme Conditions, University of Haifa.

TABLE OF CONTENTS

I. INTRODUCTION 432

II. PLURALITY OF THE STATE: THE REGULATOR 437

A. ROLES OF THE REGULATOR 438
B. PLURALITY OF (STATE) ACTORS 453

III. PLURALITY OF THE STATE: THE USER AND THE SUPERUSER 472

A. USERS 474
B. SUPERUSERS 479
1. Defining a Superuser 479
2. The State as a Cyber Superuser 482
3. The State as a Superuser in Cyber: Maintaining the Status 488

IV. REGULATING CYBER-PLURALITY 491

V. CONCLUSION 499

I. INTRODUCTION

The history of internet governance reveals an interesting story. First, there was the state, or more precisely, the United States. It founded a computer network and had sole control over it.[1] Then, the state opened the network for private use—at the infrastructure, hardware, and software levels—and took a step back while leaving further developments to market forces.[2] But the state never really left this scene, realizing that it could harness many of internet's advantages. Following the intricate process of technological evolution, social, cultural, and economic life began to transit to digital networks. As the waves of migration to the digital domain rolled (or rushed) over, the state could not allow itself to be absent. Entities began to use new technologies to digitally attack other entities, defend against such attacks, and conduct large-scale surveillance. Cyber activities—hereinafter defined as the use of digital-to-digital (D2D) transmissions in order to attack, defend, or surveil[3]—brought

1. *See* Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. 6, 7 (2003).

2. *Id.*

3. As a matter of definition, cyber activities as referred in this Article, do not capture every digital activity. As a matter of general usage, the term "cyber" is often used to describe any online activity—usually used as a prefix much like "digital," "net," "online," "E-," and "virtual"—added to an existing practice now occurring on the internet, or used as a complete

the state back to the forefront of the digital-networks scene and reshaped its role therein. To date, however, the scholarly analysis of the different roles the state plays in cyber—defined hereinafter as the medium[4] through which cyber activities are conducted—has been lagging. More specifically, little conceptual work has been done regarding the different functions the state plays in cyber; little systemic work has been made in documenting the institutional matrix with which these roles are carried out; and, consequently, little has been written on the implications of the institutional matrix and the multiple functions performed by the state on cyber governance. This Article will therefore shed important light on the distinct hats the state wears in cyber and offer preliminary recommendations that follow from such a plurality.

In a nutshell, the Article shows that the functions the state plays in cyber are more complex than one might suspect. Intuitively, one views the state as the regulator of cyber activities, regulating by setting rules, allocating liabilities, and seeking compliance. In performing this role, the state acts in its sovereign capacity, at least domestically. Whereas initially it was unclear whether the digital realm was beyond the jurisdiction of the state (and thus a sphere where freedom—or anarchy—prevails), it was soon enough established otherwise. Jurisdictional doctrines evolved,[5] and states exercised their regulatory powers—generating legal norms and enforcing them—with respect to various aspects of the cyber realm.

But "the state" is not one single entity, and digital networks cannot be compressed into just one discrete segment of social life. In fact, very few, if any, areas of social interactions remain outside the reach of digitized networks.

---

term, e.g., cybersex, cybersecurity, cyberbullying, and cyberwarfare. This Article, however, carves out a more concrete meaning for the term to set it apart for the purposes of our institutional and normative analyses. Hence, for something to be cybernetic, it must consist of Digital-to-Digital (D2D) transmission, requiring that both ends of the interaction are digital and that transmission takes place. To be considered as an activity, it must fit within one of these three categories: attack, defense, or surveillance. Thus, for the purpose of this Article, we define "cyber" activity as a D2D activity for the purposes of offense, defense or surveillance.

4. By "medium" (or dimension, or environment) we mean the physical layer (i.e., the hardware that structures the communication networks), the code (i.e., the software that enables and governs the communication), and the social context (including the economic incentives, organizational constructs, and cultural norms) within which the communication takes place. The latter infuses the technical aspect of the environment with meaning, for without recognizing the human presence (whether in the loop, on the loop, above the loop, or at the end of the loop, i.e., as an addressee) the term "cyber" is removed from the social realm of which it is a part.

5. For more on jurisdiction and territoriality on the internet, see generally DAN JERKER B. SVANTESSON, SOLVING THE INTERNET JURISDICTION PUZZLE (2017); Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L. REV. 326 (2015).

The state machinery that provides services and the regulatory regimes that oversee the provisions of goods and services therefore now interact, at least to some extent, with digitized networks. Since almost all services and almost any regulatory regimes which govern goods and services rely now on digitized networks, "the state" can be understood as a networked entity.

Such networks are vulnerable to attacks and surveillance. Some may be used as part of an offense against other states, or at least for gaining familiarity with how such services and goods provided online may be useful for those agencies in charge of offense. It is therefore not surprising to find multiple public bodies—plural segments of "the state"—performing regulatory functions that are relevant for offense, defense, or surveillance in all corners of the digital space (even if the main focus of each of these bodies is not necessarily cyber-related). As various activities migrated to the internet, various regulators began asserting jurisdiction over cyber, in line with what some have termed "regulatory capitalism."[6] As the current U.S. regulatory system reveals, a myriad of regulators at both the state and federal level are tasked with interdependently regulating cyber activities, with sometimes serpentine or crisscrossing lines of authority. Within this complex institutional matrix, it is common to find agencies resorting to regulatory tools that do not necessarily cohere with the tools used by a neighboring agency.[7]

But the plurality of the state in cyber does not stop with the plurality of regulators. The state performs two other distinct roles: a user (or client) and a "superuser" (or "superplayer"). As a user, public agencies purchase off-the-shelf and sometimes tailor-made networked products and services because without such technology, the agencies would face considerable difficulties meeting functional challenges. Today, the workflow of modern governments to a large extent relies on privately developed (and usually owned), networked products and services in a manner that not only renders these services essential across the board, but also exposes the core of the state business—the legislative, bureaucratic, and judicial functions—to cyber vulnerabilities.

6. Regulatory capitalism is the process by which the number, jurisdiction, and institutional complexity of regulatory bodies expands, the reach, depth, and intricacy (or nuance) of the regulation increases, and competition between bodies over regulatory turf and successes intensifies. *See generally* JOHN BRAITHWAITE, REGULATORY CAPITALISM (2008); Fabrizio Gilardi, *The Institutional Foundations of Regulatory Capitalism: The diffusion of independent regulatory agencies in Western Europe*, 598 ANNALS AM. ACAD. POL. & SOC. SCI. 84 (2005); David Levi-Faur, *The Global Diffusion of Regulatory Capitalism*, *598* ANNALS AM. ACAD. POL. & SOC. SCI. 12 (2005).

7. This complexity could lead to what is termed as disruptive frictions and gaps. For more on disruptive frictions and gaps in another context, see Deborah F. Shmueli, Michal B. Gal, Ehud Segal, Amnon Reichman & Evan Feitelson, *How Can Regulatory Systems Be Assessed? The Case of Earthquake Preparedness in Israel*, 25 EVALUATION 80 (2018).

Increasingly, public agencies find themselves under cyberattacks, and some have recently declared a state of emergency on account of such attacks.[8] In that respect, as customers or users, numerous public entities are dependent on networked products and services (in a rather consolidated market), which suggests that the relationship between the state as a user and the sellers and providers of these products and services is worthy of recognition and careful examination.

At the same time, the emergence of cyber activities reveals a third role of the state, "superuser." The state, given the capacities of (some of) its agencies, may affect the conduct of other players and the terms under which they operate without resorting to official powers of lawmaking and enforcement. Rather, to achieve its goals, the state may harness the unique executing powers some of the agencies possess—powers distinct from lawmaking or enforcement. Alternatively, the state may rely on the consolidation of its market share (and on its hierarchical structures necessary for such consolidation), thereby prompting all those who seek to interact with it to behave in a way the state favors. The term "superuser" therefore refers to an entity with the technical and legal capability to shape the behavior of others, control or manipulate computers and networks, and even construct, or alter, the very architecture of networks, products, or services, by *doing* or *acting*, rather than by legislating or enforcing.[9] This mode of action can take the direct form of exercising sovereign power (e.g., the state can deploy its personnel to engage directly in cyber activities) or the indirect form of private law by inserting certain demands to all contracts with state entities, designed to further its cyber policies. In practical terms, the state as a superuser has unique capabilities in attacking, defending, and surveilling (including data mining), either because of its own infrastructure, or because it can affect others to adopt certain features as a condition to conduct business with the state. Its capacity thus covers platforms (such as social networks) as well as networked devices (such as smartphones), and the capacity expands far beyond the internet.

Recognizing these three roles calls for revisiting our understanding of regulation of cyber activities. As scholars have previously noted, the state is not the sole norm-producer and enforcer in the digital world (and in other contexts).[10] These functions are also shared by other entities that may affect

8. *See, e.g.*, Kirsten Korosec, *New Orleans Declares State of Emergency Following Ransomware Attack* TECHCRUNCH (Dec. 14 2019), https://news.yahoo.com/orleans-declares-state-emergency-following-200458038.html.

9. *See infra* Part III.B.

10. The interface of law and private ordering was also examined in the corporate context. *See generally* Orly Lobel, *The Paradox of Extralegal Activism: Critical Legal Consciousness and Transformative Politics*, 120 HARV. L. REV. 937 (2007) (discussing the limits of formal law and

the behavior of many by generating social and economic norms.[11] But these entities, and such norms, are supposedly subject to state regulation themselves. If it so chooses, the state may curtail the ability of such entities to generate norms, or induce compliance with such norms, by imposing sanctions of various sorts either on the norm-generating private entities or on those who follow such norms. For example, to the extent that a platform uses its private law tools such as contracts (including complex contractual forms such as internal bylaws and terms of service) to affect the behavior of nearly all who interact with it, such contracts may be subject to legal regulation.

Yet this relationship is complex, not only because of the inherent limits of the capacity of state agencies (and their enforcement mechanisms), at least in democracies. More importantly, in the context of this Article, the state faces a dilemma precisely because the state itself is a superuser and thus affects the behavior of many others (or directly affects the architecture of the market) in a manner akin to that of private superusers. As a regulator, therefore, the state is neither merely in charge of setting the rules for the industry, nor is it concerned solely with protecting the interests of users (including itself). Rather, it also faces the dilemma of regulating itself and a small host of other entities as superusers. Viewed from the perspective of a superuser, the state is challenged with devising an interface with other superusers and securing some form of cooperation from foreign regulators, without becoming overly dependent on other superusers. At the very least, appreciating the multiple roles occupied by the state highlights the potential agency problems the state faces.

In this Article, we offer a taxonomy for better understanding the state's myriad functions in the cyber arena and further examine the possible conflicts among these functions. More fundamentally, this exercise sheds an important light on theories of state governance by elucidating the ways through which

---

the power of corporation to generate norms); *see also* Lauren B. Edelman, Linda H. Krieger, Scott R. Eliason, Catherine R. Albiston & Virginia Mellema, *When Organizations Rule: Judicial Deference to Institutionalized Employment Structures*, 117 AM. J. OF SOC. 888 (2011) (outlining the role of employers in generating norms).

11. One key example is private ordering—the sharing of regulatory authority with private actors. *See, e.g.*, Steven L. Schwarcz, *Private Ordering*, 97 NW. U. L. REV. 319 (2002); *see also* Abraham L. Newman & David Bach, *Self-Regulatory Trajectories in the Shadow of Public Power: Resolving Digital Dilemmas in Europe and the United States*, 17 GOVERNANCE 387 (2004) (demonstrating an adversarial model in the U.S., compared to a collaborative model in Europe); Luca Belli & Jamila Venturini, *Private Ordering and the Rise of Terms of Service ad Cyber-Regulation*, 5 INTERNET POL'Y REV. 1 (2016). The examination of private ordering gained momentum following Robert Ellickson work, which argued individuals often resolve disputes informally in manners that may differ from governing legal regulation. *See generally* ROBERT ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES (1991).

agencies and office holders conduct their business, either via direct action or by way of regulation. In that respect, the study of state involvement in the cyber domain is a case study through which the modern regulatory state can be better understood. Conceptually, the Article contributes to the emerging debate on the separation of powers in the digital era.[12]

The Article will proceed as follows: Part II introduces and discusses the role of the state as a regulator and the plurality of the regulators of cyber activities within the state. Part III introduces the two other roles, user and superuser, that the state plays within the plurality of cyber. In that Section, we will highlight the opposing pulls that the state faces. Part IV turns to a normative evaluation of regulation of cyber activities. The hyper-dynamic and polycentric characteristics of the domain suggests that constant oversight, agility, and collaboration—comprised of decentralization and coordination—are of particular importance in striving for a more optimal regulation. The final Section summarizes the discussion and concludes that the current roles of the state in cyber activities necessitate reexamination of both policies and governance.

II. PLURALITY OF THE STATE: THE REGULATOR

That "the state" is plural is by now understood by all.[13] It is therefore not surprising that the state acts in cyber via multiple agencies, as this Section will show. Whereas the accepted view of the state emphasizes the separation of powers between the legislature, the executive, and the judiciary, putting on the regulatory lenses brings into focus the branches functionally. While still sensitive to checks and balances, the regulatory perspective recognizes that all three branches perform a regulatory role: they formulate the rules of behavior and control enforcement of these rules as agents of the administrative state.[14]

12. *See* Yael Renan, *The Law Presidents Make*, 103 VA. L. REV. 805, 891 (2017) (arguing for the need for competent legal review of the exercise of executive power (or, by our terminology, of acting as a superuser) because governmental operations are more likely to be disclosed in the digital age); *see also* Joel Reidenberg, *Governing Networks and Cyberspace Rule-Making*, 45 EMORY L.J. 911 (1996).

13. *See generally* Eric Biber, *The More the Merrier: Multiple Agencies and the Future of Administrative Law Scholarship*, 125 HARV L. REV. 78 (2012); Jody Freeman & Jim Rossi, *Agency Coordination in Shared Regulatory Space*, 125 HARV. L. REV. 1131 (2012). This realization dates back to the legal process. *See generally* Richard B. Stewart, *The Reformation of American Administrative Law*, 88 HARV. L. REV. 1667 (1975); *see also* PETER H. SCHUCK, WHY GOVERNMENT *FAILS* SO OFTEN: AND HOW IT CAN DO BETTER (2014) (detailing thirteen different roles the state plays).

14. On the arc of policy formation and enforcement, see generally SUSAN SILBEY, ORGANIZATIONAL CHALLENGES TO REGULATORY ENFORCEMENT AND COMPLIANCE: A NEW COMMON SENSE ABOUT REGULATION (2013) (arguing that current policies and

Expanding the focus beyond administrative agencies and bureaucracy therefore necessitates recognizing the state's presence at the constitutional and statutory levels, via its constitutional organs (primarily, but not only, courts)[15] and legislative bodies (at the federal and state levels).

This Part will address the regulatory functions performed by legislatures (both primary legislatures, such as Congress and State legislatures, and secondary legislatures, such as rule-making agencies) and by courts, with respect to cyber offense, defense, and surveillance. In Section II.A we will map the challenges faced by these organs in regulating cyber activities. In Section II.B we will delve deeper into the contemporary institutional matrix in the United States, thereby providing an important dimension of the complexity (and an anchor point) for future studies of institutional design.

A. ROLES OF THE REGULATOR

The formal type of regulation by the state relies on its authority to enact legal norms, monitor compliance, and enforce deviation. As noted, this is only one segment of the larger regulatory matrix, as other bodies (e.g., industry bodies, superusers, and transnational organizations) participate in rule-making, implementation, and enforcement as well.[16] It is worthwhile, however, to focus

enforcement strategies are inconsistent, as they reflect contradicting approaches to the role of the state). In our context, the roles of the state as a user, superuser, and regulator may conflict, as the state in its capacity as a user and superuser is subject to the rules the state as a regulator enacts.

15. *See generally* MARK TUSHNET, TAKING THE CONSTITUTION AWAY FROM THE COURTS (1999) (detailing, and also arguing for, the diversification of constitutional law-making—which includes interpretation, application, and enforcement—by recognizing the role of all branches of government and multiple political and legal processes). Tushnet approaches the constitution as a "thick" complex that includes federalism, states' rights, and separation of powers. *See generally id.* Others highlight the centrality of courts at least when it comes to the "thin" constitution, namely the fundamental guarantees of equality, free speech, and liberty. *See, e.g.*, James Fleming, *Book Review: The Constitution Outside the Courts*, 86 CORNELL L. REV 215 (2001). Some have taken a stronger claim again placing judicial review at the apex of constitutional law-making. *See* LAWRENCE SAGER, JUSTICE IN PLAINCLOTHES: A THEORY OF AMERICAN CONSTITUTIONAL PRACTICE (2004); LARRY KRAMER, THE PEOPLE THEMSELVES: POPULAR CONSTITUTIONALISM AND JUDICIAL REVIEW (2004); *see also* James Fleming, *Judicial Review without Judicial Supremacy: Taking the Constitution Seriously Outside the Courts*, 73 FORDHAM L. REV. 1377 (2004). For a law-and-society perspective on the recourse to courts, see Emily Zackin, *Popular Constitutionalism's Hard When You're Not Very Popular: Why the ACLU Turned to Courts*, 42 L. & SOC. REV. 367 (2008).

16. For an interesting empirical analysis of the interaction of the various regulatory processes and actors, see Michael W. Toffel, Jodi L. Short & Melissa Ouellet, *Codes in context: How states, markets, and civil society shape adherence to global labor standards*, 9 REGULATION & GOVERNANCE 205 (2015).

on the state, because it has the formal power to structure the playing field within some political and economic parameters.

The basic paradigm within which the state operates is premised on the well-known tension between *governability*, namely the desire to empower the state to effectively address harms and risks, and *limited government*, namely the desire to check the power of the state via mechanisms of separation of powers. Substantively, the checks are not merely about empowering different entities so that they may counter each other, but rather seeking a balance between the promotion of the public interests and the protection of rights (and liberties) through processes that are committed to representation, participation, and accountability. This basic structure was incrementally developed in the nineteenth century, adjusted in the New Deal era (with the lessons of the *laissez-faire* regime of the industrial revolution in mind), recalibrated in the 1960s (with the lessons of segregation in mind), and then reenvisioned by Neo-liberal deregulatory pressures.[17] It is now facing the ascendancy of the data revolution of the twenty-first century, which disrupts past equilibria.[18]

At the very least, the emergence of the networked ecosystem (and the economics of surveillance capitalism)[19] challenges the dominant paradigm that highlights the importance of separation of powers. The networked ecosystem is premised on a relatively clear logic of amalgamating all forms of data collection and analysis, and revolves towards the consolidation on account of the network effect.[20] Faced with such centripetal forces that apply on business and government alike, attempts to bifurcate power—regulatory and economic—confronts mounting counter-pressures. It is more difficult for the regulator to split a data giant (such as Microsoft, Google, or Facebook). In addition to possessing substantial capital and lobbying capabilities, these giants would, on the merits, point to the desirability of allowing data and analytic tools to converge and thereby generate greater welfare to society. In light of

17. For the historical evolution, see SILBEY, *supra* note 14.

18. Orin Kerr identified a dynamic he calls an "equilibrium-adjustment"—"a judicial response to changing technology and social practice." Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011).

19. *See generally* SHOSHANA ZUBOFF, THE AGE OF *SURVEILLANCE* CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2018) (demonstrating how data has emerged as a new form of capital, generating production lines of data and structures of surveillance and analysis, premised on the economic value that can be extracted by data collection, mining, and algorithmic analysis).

20. Notably, in a federal state like the United States, the two levels of government must also be engaged. *Cf.* Daniel Abebe, *Cyberwar, International Politics and Institutional Design*, 83 U. CHI. L. REV. 1 (2016); Ashley Deeks, *Checks and Balances from Abroad*, 83 U. CHI. L. REV. 65 (2016); Jon Michaels, *Separation of Powers and Centripetal Forces: Implications for the Institutional Design and Constitutionality of Our National Security State*, 83 U. CHI. L. REV. 199 (2016).

such convergence, similar pressures apply on the state machinery. It is more difficult to insist on separating state powers in the face of ever-growing and fast-developing threats (emanating from conglomerated opponents and diffuse networks of hackers alike). Preparedness, response, and recovery from such threats requires a greater degree of coordination among the various state agencies and between the legislature, the courts, and the executive. But on a deeper level, the state itself faces pressures to amalgamate data and produce better analytic tools, regardless of whether the data was generated or produced by an action of an executive agency, a legislature or a court, and regardless of whether it can be used later by a policy maker, a legislator, or a judge. In other words, as the economy moves towards adopting algorithm-based predictive tools, so does the state. Consequently, without forsaking the differentiated functions of legislatures, courts, and bureaucracies, a collaborative approach[21] might be a better way to understand cyber-related separation of powers. As will be shown in this subsection, this is not a minor challenge given the contemporary institutional design.

But before this claim is further developed, a quick word on terminology. While some view the term "regulation" as distinct from primary legislation,[22] this distinction is less relevant to the extent that this Article's focus is on the substance of the legal norms that govern a certain field, rather than the internal hierarchy of the governing norms. The distinction between primary statutes and secondary (or tertiary) rule-making powers, however, may still be helpful in so far as it highlights the different challenges faced by the primary legislature (Congress or state legislatures) versus those faced by the secondary (or tertiary) rule-maker (such as departments of the government or agencies at the federal or state levels). To the extent that the statutory regime is designed to include norms at a more general level of abstraction—the principles which empower secondary and tertiary bodies to enact secondary and tertiary norms—and to the extent that amending legislation is more difficult in terms of political resources and time than amending secondary rules, one would expect the legislature dealing with cyber activities to delegate significant rule-making authority to the ostensibly more agile and responsive agencies. However, such a move may present a dilemma since such authority may lack sufficient checks

21. *See generally* AILEEN KAVANAGH, THE COLLABORATIVE CONSTITUTION (2018).

22. *See* David Levi-Faur, *Regulation and Regulatory Governance* 8 (Jerusalem Papers in Reg. & Gov., Working Paper No. 1, Feb. 2010), http://levifaur.wiki.huji.ac.il/images/Reg.pdf ("[R]ules will be considered as regulation as long as they are *not* formulated directly by the legislature (primary law) or the courts (verdict, judgment, ruling and adjudication). In other words, regulation is about bureaucratic and administrative rule making and not about legislative or judicial rule making."). Levi-Faur admits that in other contexts, regulation could be defined differently. *See, e.g.*, *id.* at 5, 8–9 (author recognizes other approaches).

and balances on the discretion of the agencies. Primary legislation is not only about empowerment, but also about confining secondary and tertiary rule-making power. Still, defining—at the statutory level—attack, defense, and surveillance to a sufficient degree of specificity is difficult, if only because the technology evolves at a rapid or even hyper-rapid rate. Ever more devices and human practices are being networked; offense, defense, and surveillance tools are expanding; and the potential boundaries between the digital and the biological (human) realms may themselves become permeable. It is therefore worthwhile to examine in greater detail the frameworks that the primary legislatures set up at the federal or state level.

These frameworks need to make sense in terms of the level of specificity located at the statutes versus the scope of the rule-making power located at the agency or sub-agency level. The greater the specificity, the greater the check is on the agency as an expression of the primary legislative power vested in the legislature. However, such specificity may hamper governability because the expertise and responsiveness usually lie with the agencies. Yet, the framework must also make sense in terms of its coherency with the norms of other jurisdictions, at the statutory or sub-statutory levels, as the modern economy and cyber activities in particular are transnational in nature. Such a framework may include specific rules of do's and don'ts, or may opt for stating broader principles and delegating rule-making power to other entities.[23] These entities, in turn, are entrusted with gathering and sharing information (*inter alia*, for conducting audits), enforcing the do's and don'ts, or translating the broader principles to concrete and enforceable measures by issuing bylaws (i.e., regulations, guidelines, circulars, policies, or other documents that carry varying degrees of legal forces, from being fully binding as a matter of formal law, to conveying recommendations, albeit with a practical force similar to binding norms).

While a statutory framework is the basic foundation of a regulatory regime, its reliance on the party-political process is yet another reason to recognize the importance of sub-statutory mechanisms. Viewed from this angle, to the extent that the sub-statutory rules are a product of professional discourse (or, at least, a product of discourse more influenced by professional reasoning), this level of legislation can be seen as part of the checks and balances necessary for addressing some of the potentially sub-optimal outputs of party-political bargaining.[24] This, of course, is not to say that agency-generated rules are free

23. *See* 5 U.S.C. § 553 (2012) (setting the rules for rule-making).

24. Such suboptimal outputs include the inability to reach a political compromise for reasons not directly related to the subject matter at hand or because the party-political process may be subject to forms of capture by special interests through lobbying and campaign finance.

from capture. Special interests may apply pressures either through offering agencies' personnel lucrative post-employment options, applying pressure on the politics of appointments of key agency figures, or exerting pressure through lobbying (at the agency and legislative level). Such pressures may be directed at the rule-making, budget, and enforcement policies, and may be supplemented with threats of litigation.

Nevertheless, as a general matter, capturing all the relevant agencies and the legislature is—one can only hope—more difficult. From the perspective of checks and balances, a distribution of powers and functions is therefore preferable, provided a degree of coordination is maintained. However, this coordination is not easy to generate, both because of the multitude of agencies (as will be discussed below) and because of the blurred boundaries and cross-impacts between regulatory regimes. Whereas a statutory framework may be direct in the sense that the legislature (e.g., Congress or state legislators)[25] passes various bills governing cyber activities,[26] it could also be indirect, involving activities that are only remotely linked to cyber but may nonetheless have an impact on the domain.

With this in mind, the choices facing the legislature in regulating cyber activities must be addressed more specifically. First is the challenge of defining

For more on capture in the cyber-context, see generally David Thaw, *Enlightened Regulatory Capture*, 89 WASH. L. REV. 329 (2014).

25. For a full updated list of all U.S. state statutes regarding computer hacking and unauthorized access, see *Computer Crime Statutes*, NAT'L CONF. ST. LEGISLATURES, http://www.ncsl.org/issues-research/telecom/computer-hacking-and-unauthorized-access-laws.aspx (last visited July 20, 2019).

26. Congress enacted various laws that relate to cyber activities. *See, e.g.*, Electronic Communications Privacy Act (ECPA) of 1986, Pub. L. No. 99–508, 100 Stat. 1848 (1986). The ECPA provides, *inter alia*, criminal sanctions and civil remedies for the unauthorized interception or disclosure of electronic communications. *See generally id.* The Computer Fraud and Abuse Act (CFAA) also provides criminal sanctions and civil remedies to various cyber activities, e.g., intentionally accessing a computer without authorization and exceeding authorized access of a protected computer. *See* Computer Fraud and Abuse Act of 1986, Pub. L. No. 99–474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030 (2012)).

a cyberattack,[27] including the exceptions[28] pertaining to a justifiable or excusable cyberattack (domestically and internationally).[29] Such an approach will have to confront the substantive questions: What is an attack? What counts as consent, and does consent necessarily negate an attack? Are attacks always wrong, or are some self-defense or preemptive measures justified? Is there a difference between a state-led attack and a superuser-led attack (assuming that the state and other superusers may resort to similar methods)? These questions are further complicated by institutional challenges. For instance, one might ask. Which agency has the authority to identify attacks and decide on their permissibility? Under such a form of regulation, legislators set the rules of cyberattacks. Violating the rules by attacking outside the scope of an exception will most likely be subject to civil and/or criminal liability. In such circumstances, users or superusers (agents of the state included) could face sanctions.

A different path, which may be used as an alternative, is to regulate technology. The legislature can shape cyber activities by deciding which networks could be used, by whom, how, and for what purposes. They could restrict the use of risky, or outdated, hardware, software, and networks by either code or by imposing liability for using them.[30] Under this approach,

27. Defining a "cyberattack" is not an easy task, both in domestic and international laws. Offering a taxonomy of cyberattacks, scholars proposed that "A cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose." Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 826 (2012). On the international level, the latest edition of the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* defines a "cyber-attack" as a "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects." *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2d ed. 2017).

28. *See generally* Richard Epstein, *Government by Waiver*, 7 NAT. AFF. 39 (2011); Stephen Breyer, *Analyzing Regulatory Failure: Mismatches, Less Restrictive Alternatives, and Reform*, 92 HARV. L. REV. 549, 569 (1979); Carry Coglianese, Gabriel Scheffler & Daniel Walters, *The Hidden Face of Power and Discretion in the Administrative State* (manuscript with authors).

29. Acts of retaliation are also considered as a form of attack, although they could be categorized as defense measures. Such retaliation acts could be done by both users and superusers, and they are not merely due to the attacks on them, but also due to attacks on others. When Sony was attacked, U.S. President Barack Obama vowed to mount a "proportional" response against North Korea, although the attack was not against the state *per se*. *See* Dave Boyer, *White House threatens 'proportional' response to North Korea cyberattacks on Sony Pictures*, THE WASH. TIMES (Dec. 18, 2014), http://www.washingtontimes.com/news/2014/dec/18/white-house-threatens-proportional-response-north-/?page=all. For more on acts of retaliation in cyber, see generally Eldar Haber, *The Cyber Civil War*, 44 HOFSTRA L. REV. 41 (2015).

30. See, for instance, how the United States decided to ban federal agencies from buying Huawei's products, claiming it poses security threats. *See* Raymond Zhong, *'Prospective Threat'*

certain technologies could be labeled as weapons or certain networks as no-access or highly limited access spaces, and thus the use of such weapons or unauthorized access can be defined as an attack, and the possession of such weapons could form a distinct form of liability.

Next is cyber defense.[31] Much like cyberattacks, regulators can set ground rules for cyber defense against domestic and international threats. Defense can be both passive and active.[32] Passive defense refers mostly to security measures and includes three general types: requiring that specific codes or hardware be adopted; stating the qualifications cyber-security personnel must meet as well as the requirement to include such positions in regulated entities; and outlining the workflow processes that each regulated entity must implement. Explicitly prescribing the tools that entities must adopt in order to avoid a sanction (or the tools they may adopt in order to receive a benefit) is designed to prevent exploitations of known weaknesses. Detailing the accreditation of personnel that such entities must or may employ (and in what capacities) is aimed to ensure the capacity of the entities to adapt to evolving threats. Outlining the ongoing processes that entities must or may undertake adds an element of organizational learning (from best practices and past failures) and allows for inter-operability by ensuring similar-enough operational language across entities. Regulating the specific tools often addresses encryption, firewalls, and automated detection.[33] Regulating personnel could include mandatory requirements of employees' credentials that prove, *inter alia*, knowledge and expertise.[34] Regulating processes includes information sharing,[35] education,

of Chinese Spying Justifies Huawei Ban, U.S. Says, N.Y. TIMES (July 5, 2019), https://www.nytimes.com/2019/07/05/technology/huawei-lawsuit-us-government.html.

31. A rather traditional form of cyber defense is the use of virus-scanning software or firewalls designed to protect computers from unauthorized adversaries. But antivirus software can itself serve as a spyware because it has ongoing access to all files and folders. Similarly, firewalls may include back doors. For more on antiviruses that might contain spyware, see Brain Barrett, *Most Android Antivirus Apps are Garbage*, WIRED (Mar. 16, 2019), https://www.wired.com/story/android-antivirus-apps-bad-fake.

32. *See* Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 230 (2002).

33. For a detailed mapping of encryption laws and policies worldwide, see *World map of encryption laws and policies*, GLOBAL PARTNERS DIGITAL, https://www.gp-digital.org/world-map-of-encryption/ (last visited July 20, 2019).

34. See, for instance, the Global Information Assurance Certification (GIAC), which validates the skills of information security professionals and provides "assurance that a certified individual has the knowledge and skills necessary for a practitioner in key areas of computer, information and software security." *About: Program Overview*, GIAC, https://www.giac.org/about/program-overview (last visited July 20, 2019).

35. One key example is Computer Security Incident Response Teams (CSIRTs), sometimes also referred to as Computer Emergency Response/Readiness Teams (CERTs),

and facilitating recovery from attacks.[36] Active defense is both preventative and reactive; conceptually, it also covers those three axes of tools or measures, personnel, and processes. As such, it refers to detecting, tracing, and perhaps even actively responding to threats.[37]

Finally, there is the issue of cyber surveillance. By legislative acts—subject to judicial interpretation (and constitutional judicial review), which will be further addressed below—the regulator decides what counts as surveillance, whether surveillance is permitted, by whom, under which circumstances, and whether to institute procedures to ensure safeguards for entities against unauthorized surveillance. Both users and superusers (state agencies or otherwise) could be subject to surveillance, and both, in theory, may seek authorization to conduct surveillance. Companies, which could act as both users and superusers, could be barred from collecting and retaining data, or at least their legal ability to do so may be limited.[38] Alternatively, entities may

---

which handle computer security incidents within an institution and many times also operate at the national level. Among the many roles these teams assert, e.g., providing cybersecurity and infrastructure security knowledge and practices to its stakeholders, they usually promote information sharing between private and public entities. For more on CSIRTs, see Robert Morgus, Isabel Skierka, Mirko Hohmann & Tim Maurer, NATIONAL CSIRTS AND THEIR ROLE IN COMPUTER SECURITY INCIDENT RESPONSE (Nov. 2015), http://www.digitaldebates.org/fileadmin/media/cyber/National_CSIRTs_and_Their_Role_in_Computer_Security_Incident_Response__November_2015_--_Morgus__Skierka__Hohmann__Maurer.pdf. Another example is the Cybersecurity Information Sharing Act, which authorizes, *inter alia*, private entities to monitor their information systems, operate defensive measures, and share "cyber threat indicators" or "defensive measures" for a cybersecurity purpose. Consolidated Appropriations Act of 2016, Pub. L. No. 114–113, § 104(c)(1), 129 Stat. 2242 (2016) (codified as amended at 6 U.S.C. §§ 1501–10 (2012 & Supp. Ill 2016)).

36. *See* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 471 (2012).

37. *Id.* at 460–70.

38. One key example is the European Union, which imposes certain limitations and restrictions on data collection by companies in some circumstances under its General Data Protection Regulation (GDPR). These include, *inter alia*, purpose specification (personal data must be collected for a "specified, explicit and legitimate" purpose and cannot be further "processed" in a way which is "incompatible" with such original purposes) and data minimization (data must be "limited to what is necessary in relation to the purposes for which they are processed"). Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Advancement of Such Data, and repealing Directive 95/46/EC, art. 5, 2016 O.J. (L 119) 35. For more on the GDPR, see generally Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995 (2017). An example of data limitation can also be seen in the United States within the California Consumer Privacy Act (CCPA), which goes into effect January 1, 2020. Among other things, the CCPA excludes the collection and sale of "a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California," where "commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside

receive authorization or even a mandate to do so.[39] The regulator, usually in primary legislation, could determine how data should be collected, for how long it could be retained, and under which circumstances the industry can use or trade it. In this instance, limitations could be specific. For example, the regulator can limit usage of the data for specific purposes, such as targeted marketing. It could also set limitations on transferring or selling data to the state and/or other states.[40]

Related is the question of state surveillance. The regulator can decide the manner in which the state executes its surveillance capabilities. Much like with companies, the regulator could bar the state from any acts of surveillance. But more likely, the regulator will set a legal framework that requires the state to act in order to conduct surveillance.[41] Thus, even if the legislature bars the state

---

of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold." Cal. Civ. Code § 1798.145(6) (2018).

39. Unlike the European Union, in which many countries mandate Internet Service Providers (ISPs) to collect and retain data on their customers, the United States has not yet implemented mandatory data retention requirements. An exception is set under the Stored Communications Act, where providers of electronic communications or remote computing services store electronic communications or communications records could be asked upon a governmental request to preserve stored data for up to 180 days. *See* 18 U.S.C. § 2703 (2012). For more on data retention, see generally Catherine Crump, *Data Retention: Privacy, Anonymity, and Accountability Online*, 56 STAN. L. REV. 191 (2004); *see also Mandatory Data Retention*, EFF, https://www.eff.org/issues/mandatory-data-retention/us (last visited July 20, 2019).

40. While setting few exceptions, the Stored Communications Act prohibits providers of remote computing service or electronic communication services from voluntarily and knowingly divulging a record or other information pertaining to a subscriber or a customer of such service to any governmental entity. *See* 18 U.S.C. § 2702 (2012). As for non-voluntary disclosure, in order to obtain customer communications or records by companies, the state is required to obtain a warrant, present an administrative or grand jury subpoena (with notice to the subscriber), or obtain a court order for disclosure (with notice to the subscriber). *See* 18 U.S.C. §§ 2703(a)–(b) (2012).

41. Regulation of state surveillance in the United States began under the Omnibus Crime Control and Safe Streets Act. This Act permitted surveillance for national security purposes, *see* 18 U.S.C. § 2511(3) (1970), while conditioning the usage of electronic surveillance to judicial finding of a probable cause to believe the target is committing, has committed, or is about to commit a particular enumerated offense, and that the surveillance would obtain incriminating communications about the offense. *See* 18 U.S.C. § 2518(3) (1970); *see also* Caitlin Thistle, *A First Amendment Breach: The National Security Agency's Electronic Surveillance Program*, 38 SETON HALL L. REV. 1197, 1200 (2008). In 1978, Congress enacted the Foreign Intelligence Surveillance Act (FISA), regulating electronic surveillance of American citizens or permanent residents within the United States for foreign intelligence or international counterterrorism purposes. *See* Pub. L. No. 95–511, 92 Stat. 1783 (1978). Under FISA, the state requires Foreign Intelligence Surveillance Court (FISC) approval prior to conducting surveillance on Americans. 50 U.S.C. § 1805 (2012). Congress broadened the state's ability to conduct surveillance in the aftermath of the September 11 attacks. First, the Terrorist Surveillance

from conducting surveillance, it could allow companies to transfer data to the government[42] or even mandate such data disclosure.[43]

With variations in legal systems, and notwithstanding judicial rhetoric to the contrary, the judiciary could also act as a regulator. Judges settle disputes by following the rules set by the legislature or the agencies. Upon closer look and to the extent that regulation is approached from the perspective of the subject matter, however, adjudication is a component of regulation as judges interpret the law and infuse it with concrete, practical meaning each time they apply it.[44] This may entail not only striking down legislation that conflicts with

---

Program (TSP) enabled the "intercept[ion of] international communications into and out of the United States" by persons linked to terrorist organizations. Edward C. Liu, *Reauthorization of the FISA Amendments Act*, CONGRESSIONAL RESEARCH SERVICE, at 4 (Apr. 8, 2013), http://www.fas.org/sgp/crs/intel/R42725.pdf. Mainly, however, Congress enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA Patriot Act"), which added Section 215 to FISA. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, Pub. L. No. 107–56, § 215, 115 Stat. 272 (2001). Section 215 allowed the director of the FBI, or a designee of the director under a FISC order, to compel telecommunications providers to produce metadata. 50 U.S.C. § 1861(a)(1) (2012). Section 215 expired on June 1, 2015. One day after, Congress passed the USA Freedom Act, which, *inter alia*, amended the bulk data collection set by Section 215 to authorize collection from phone companies of up to "two hops" of call records related to a suspect when the government can prove it has "reasonable" suspicion that the suspect is linked to a terrorist organization. *See USA Freedom Act: What's in, what's out*, WASH. POST (June 2, 2015), https://www.washingtonpost.com/graphics/politics/usa-freedom-act/. In 2007, Congress enacted the Protect America Act (which replaced the TSP), amending FISA by, *inter alia*, increasing the state's ability to conduct surveillance on foreign communications, where one party is reasonably believed to be outside of the United States. *See* Protect America Act, sec. 2, § 105A, 121 Stat. 552, 552 (2007). In 2008, Congress enacted the FISA Amendments Act of 2008 (FAA), which added Section 702, allowing to intercept content and adding a new procedure for internet and telephone content surveillance without individualized court orders for targeting non-U.S. persons abroad. *See* Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110–261, 122 Stat. 2436 (2008). For more on U.S. surveillance legislation, see G. Alex Sinha, *NSA Surveillance Since 9/11 and the Human Right to Privacy*, 59 LOY. L. REV. 861, 873–74 (2013); Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1 (2008).

42. For more on data sharing within public-private partnerships under national security regulation, see generally Niva Elkin-Koren & Eldar Haber, *Governance by Proxy: Cyber Challenges to Civil Liberties*, 82 BROOK. L. REV. 105 (2016).

43. For more on regulation through disclosure, see generally Cass R. Sunstein, *Informational Regulation and Informational Standing: Akins and Beyond*, 147 U. PA. L. REV. 613 (1999).

44. *See* Malcolm Feeley & Ed Rubin, *Prison Litigation and Bureaucratic Development*, 17 LAW & SOC. INQUIRY 125 (1992) (showing how courts played a major role in reforming prisons in the United States); Malcolm Feeley & Ed Rubin, JUDICIAL POLICY MAKING AND THE MODERN STATE: HOW THE COURTS REFORMED AMERICA'S PRISONS (1998) (also showing how courts played a major role in reforming prisons in the United States). In the United States,

constitutional norms (e.g., regarding separation of powers between the branches, federalism, or rights),[45] but also reading it so as to minimize constitutional conflicts.[46] Equally, if not more importantly, judges have a role to play in cases where legal norms are insufficiently clear.[47] In cases that end up litigated, such uncertainties regarding legal norms are part of the reasons for litigation (together with factual disputes, which may themselves raise legal questions regarding procedure and evidence—matters highly relevant for cyber-related disputes). In that respect, adjudication generates practice and, in common law systems, precedent. Therefore, jurisprudence is a necessary component of regulation.

Such form of regulation applies also to all three components of cyber activities. In all three components, courts could decide on the lawfulness of a state's action (and, of course, actions of other users and superusers within the

---

the debate regarding the extent to which courts should defer to agencies in interpreting statutes is very much alive. *See infra* note 47.

45. On the contested constitutionality of cyber statutory measures, see generally Peter Margulies, *Defining Foreign Affairs in Section 702 of the FISA Amendments Act: The Virtues and Deficits of Post-Snowden Dialogue on U.S. Surveillance Policy in the Post-Snowden Age*, 72 WASH. & LEE L. REV. 1283 (2015). For a claim that the amendment of the FISA Act of 2015 weakens privacy and civil liberties by being overbroad, see generally Coalition Letter to Senate Leadership in Opposition to drafted FISA Improvements Act of 2015 and the FISA Reform Act of 2015 (May 28, 2015), https://alair.ala.org/handle/11213/948. On the role of courts, see generally MARTIN SHAPIRO, LAW AND POLITICS AND IN THE SUPREME COURT (1964) (showing how judges navigate between substantive and institutional questions in deciding whether to intervene in the decisions of other branches); MARTIN SHAPIRO, COURTS: A COMPARATIVE AND POLITICAL ANALYSIS (1986) (showing the various functions courts perform in different constitutional systems, and highlighting the potential difference between rights-based and federalism-based judicial review).

46. This is pursuant to the constitutional avoidance doctrine, which states that "[w]hen the validity of an act . . . is drawn in question, and even if a serious doubt of constitutionality is raised, . . . [the] Court will first ascertain whether a construction of the statute is fairly possible by which the question may be avoided." Ashwander v. Tenn. Valley Auth., 297 U.S. 288, 348 (1936) (Brandeis, J., concurring). For further reading on the constitutional avoidance doctrine, see generally Andrew Nolan, *The Doctrine of Constitutional Avoidance: A Legal Overview*, CRS REPORT 7–5700, 1 (Sept. 2, 2014), https://fas.org/sgp/crs/misc/R43706.pdf; Lisa A. Kloppenberg, *Avoiding Constitutional Questions*, 35 B.C. L. REV. 1003 (1994); LISA A. KLOPPENBERG, PLAYING IT SAFE: HOW THE SUPREME COURT SIDESTEPS HARD CASES AND STUNTS THE DEVELOPMENT OF LAW (2001).

47. See, for instance, the Chevron deference doctrine, by which federal courts, when reviewing a federal government agency's action, must defer to the agency's construction of a statute that Congress directed the agency administer. *See Chevron U.S.A., Inc. v. Nat. Res. Def. Council, Inc.*, 467 U.S. 837 (1984). *But see PDR Network, LLC v. Carlton & Harris Chiropractic, Inc.*, 139 S. Ct. 2051 (2019) (discussing courts' power to review agency rules under the FCC's interpretation of the Telephone Consumer Protection Act); *Kisor v. Wilkie*, 139 S. Ct. 2400 (2019) (regarding the interpretation by an executive agency of its own regulations).

regulatory framework).[48] For example, using their interpretation of existing legislation could lead to banning the distribution or application of certain segments of technology (e.g., due to intellectual property infringement or any other relevant legislative act).[49] In the cyber realm, court decisions could regulate the fields of attack, defense, and surveillance through legally channeling the development of the architecture (i.e., code). The court may thus place limits on certain technologies by elucidating the boundaries between the permissible and the impermissible. Needless to mention, courts also decide on the constitutionality of the acts, thereby holding a veto power within the overall regulatory design. Such veto power may result in striking down a certain regulatory mechanism in favor of a previous one, or in shaping the regulation by either interpreting the act so as to comply with the constitution or including language that will guide (or, in some jurisdictions, nudge or even prompt) the law maker towards a constitutionally acceptable form of regulation.

Beyond legal precedents, courts could also regulate cyber through their decisions regarding compliance or noncompliance with governmental requests or decrees regarding surveillance.[50] And of course, adjudication casts a

48. Private entities could also act as regulators. A good example is the Internet Corporation for Assigned Names and Numbers (ICANN), which was once governmentally owned and privatized. ICANN controls domain names on the internet and ensures the network is stable, regulating mainly through bylaws. *See Bylaws for Internet Corporations for Assigned Names and Numbers*, ICANN, https://www.icann.org/resources/pages/governance/bylaws-en (last visited July 20, 2019).

49. In the famous *Napster* decision, the court impacted the evolution of file-sharing technology by ruling on the relationship between the technology and the protected content. *See generally A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (2001). But we could think of other examples where technological components are directly subject to intellectual property and the rightsholder prevents others from using such components even when the rightsholder refrains from using them. However, generally speaking, the typical intellectual property protection covers technology already in use by the rightsholder. This may be distinct from other legal regimes, where technology itself, such as forms of encryption, missile guidance, or malware, is restricted, and the courts play a role in determining whether a certain case falls within that restriction. But on second thought, it is usually the case that at least the state, if not other superusers, generate some exceptions to the development and application of restricted technology, and so the logic of the regime of intellectual property is not radically different from the logic of a restricted technology regime when viewed from a regulatory perspective (and the role of courts therein).

50. In the United States, the Foreign Intelligence Surveillance Court (FISC) plays a crucial role in deciding whether the government receives data and metadata on civilians. As we came to learn, mainly from Edward Snowden's revelations in 2013, FISC judges often approved blanket orders, as requested by governmental agencies, to obtain metadata on American citizens. *See* Elkin-Koren & Haber, *supra* note 42, at 148, 153–54. While Congress is responsible for the creation of FISC and Section 215 of the USA Patriot Act, 50 U.S.C. § 1861 (2012), which enabled FISC judges to approve surveillance requests, their decisions on this matter shape the state's ability to perform legal surveillance. Therefore, Congress's rulings

"shadow" that guides enforcement agencies in conducting their business and companies in directing their compliance practices.[51] As part of its role in enforcement, the judiciary regulates cyber behavior by issuing sentences, which must, at least in the United States, comply with relevant guidelines. Such sentencing guidelines in the United States are issued by the U.S. Sentencing Commission (USSC), an independent agency within the judicial branch of government.[52] By establishing sentencing policies and practices for the federal courts, and by advising and assisting Congress and the executive branch, the USSC decides how federal courts implement cyber-related legislation. Therefore, the USSC could shape cyber activities in its regulatory capacity.[53] In cases of cyber, enforcement is also complicated because of the trans-jurisdictional dimension of these activities, as other judiciaries may follow different guidelines.

The multiplicity of courts, procedures, and evidentiary rules raises a challenge. It is an important component of the constitutional structure that is designed to separate powers and functions so that no governmental agency, including courts, could amass sufficient capability to capture the others.[54] But to the extent a fundamental element of social life—and in our case, technology—evolves in a manner that ostensibly requires the state to develop greater coordination among its subcomponents in order to avoid a breach (or a capture) of the weakest link, the multiple breaks and leverages built into the system may prove suboptimal. This is so not because the idea of checks and balances has outlived its usefulness. On the contrary, it is ever more relevant, given the risk of over-concertation embedded in far-reaching digitized

---

could shape conduct. *See* Conor Clarke, *Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp? Ex Parte Proceeding and the FISC Win Rate*, 66 STAN. L. REV. ONLINE 125, 126 (2014). For more on government's success rate in FISC proceedings, see, for example, *Continued Oversight of the Foreign Intelligence Surveillance Act: Hearing Before the S. Comm. on the Judiciary*, 113th Cong. 49 (2013) (containing a statement of Laura K. Donohue, Professor, Georgetown University Law Center), *available at* http://scholarship.law.georgetown.edu/cong/117 (arguing that the "rather remarkable success rate" raises a "serious question about the extent to which FISC and [the Foreign Intelligence Surveillance Court of Review] perform the function they were envisioned to serve"); Theodore W. Ruger, *Chief Justice Rehnquist's Appointments to the FISA Court: An Empirical Perspective*, 101 NW. U. L. REV. 239, 245 (2007) (arguing that the "government success rate [is] unparalleled in any other American court").

51. *See generally* Robert H. Mnookin & Lewis Kornhauser, *Bargaining in the Shadow of the Law: The Case of Divorce*, 88 YALE L.J. 950 (1979) (discussing the impact of the legal system on negotiations and bargaining that occur outside the courtroom).

52. *See About*, USSC, http://www.ussc.gov/about (last visited July 20, 2019).

53. *See id.*

54. The Framers had in mind harnessing diverging incentives so that ambition (to amass power and control) will counteract ambition (of others to do the same). *See* THE FEDERALIST NO. 51 (James Madison).

networks coupled with strong computers and sophisticated software. But the judicial technology that underlies the regulatory function performed by courts—consisting of jurisdictional boundaries, time-consuming motions, and discovery and evidentiary hearings split among various courts—was originally designed with 18th century technology in mind and was updated in the 1940's in the aftermath of the New Deal, itself a product of the Industrial Revolution and the need to rearrange the State (including courts) so as to check against market pressures. It is not clear that this design places courts in a sufficiently optimized position to perform their regulatory function in our contemporary, networked economy, when we have offense, defense, and surveillance activities in mind.

On a more general level, even before we address the executive branch in greater detail, this analysis reveals that the traditional separation of state powers into three branches—the legislative, executive, and judicial—offers a less helpful lens for understanding the regulatory challenges faced by the state, as each branch regulates in their own way. A more helpful way to approach the challenges is, therefore, to focus on the field itself—namely offense, defense, and surveillance. Here, two main challenges face the state in its regulatory capacity (exercised via the primary legislature, the secondary rule-maker, or the courts). The first is the hyper-dynamic progress of technology. The second is the dynamic transfer of knowledge and people among organizations, entities, and jurisdictions. With this in mind, the state has to determine the applicable norms by defining the identity of those subject to regulation. Are they individual users? Commercial and nonprofit enterprises? Government users/superusers? Or are they rather only operators and owners of critical infrastructure (and if so, how is that category defined)? Again, as stated, since the state is not monolithic, public regulators may, as a matter of course, issue a regulation to which other segments of the state are subject (provided the latter are subject to the jurisdictions of the former). Alternatively, the regulation may address the industry—namely the entities that develop the hardware and software—either by way of rules or by way of guidelines. The regulation also has to determine the point of interaction, or node within the social or economic nexus, where the regulation applies, such as the purchase/

sale of certain software or hardware, its usage,[55] or its export/import.[56] Lastly, the regulator must decide on the modality of regulation. For example, the regulator may decide to regulate through information[57] or focus on granting the executive the authority to execute an internet "kill switch" under some circumstances.[58]

---

55. Considerably, the regulator can determine the architecture of digital technology and networks. There are various methods to achieve control over design, the first of these methods being through hardware. The state could regulate both domestic and international manufacturing of hardware. On the international level, the state could determine which hardware enters its domain. If the United States suspects that China places surveillance equipment in its hardware, it might restrict any entry of China's hardware into the United States by legislation. *E.g.*, *supra* note 30. The regulator could also deploy other means of restrictions like, for example, technological standards. The state can determine that only hardware satisfying a pre-determined set of standards can enter and/or be used in the United States. Similarly, those same rules could apply to domestic manufacturers and/or suppliers. Second, the state can regulate software. Much like the hardware industry, the state can regulate computer software, and computer software is not limited to traditional computers. There are many appliances and devices that use computer software, such as televisions, washing machines, refrigerators, and many more. With the developments of the Internet-of-Things (IoT), all such appliances might be subject to cyberattacks and/or surveillance. For more on Internet of Things, see, for example, Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85 (2014).

56. *See, e.g.*, Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (July 12, 1996), www.wassenaar.org (a multilateral export control regime intended to promote transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies).

57. This can be done, for example, by requiring information sharing and/or notification of data breach. *See infra* note 136.

58. An internet "kill switch" usually refers to a government's ability to disconnect the country, or part of it, from the internet. Naturally, it does not refer to a physical switch, but rather to an ability to order ISPs to cease communications. An example of such a kill switch can be traced in 2011, in Egypt, in which the government darkened the internet domestically. *See The Day That Egypt Unplugged the Internet*, WSJ BLOGS: DISPATCH (Jan. 28, 2011, 11:29 AM), http://blogs.wsj.com/dispatch/2011/01/28/the-day-that-egypt-unplugged-the-internet. Similar incidents occurred in other countries as well. *See* Jonathan Zittrain & Molly Sauter, *Will the U.S. Get an Internet "Kill Switch"?*, TECH. REV. (Mar. 4, 2011), http://www.technologyreview.com/web/32451/?mod=chfeatured&a=f (describing internet shut-downs in Nepal and Burma). In the United States, the existence of an internet kill switch is debatable. Few argued the United States already has such a kill switch under the Communications Act of 1934 because Section 706 of the Act, as amended in 1941, grants the U.S. President an authority to shut down "any facility or station for wire communication . . . ." Communications Act of 1934, Pub. L. No. 73–416, § 706(d), 48 Stat. 1064 (1934) (codified as amended as 47 U.S.C. § 606 (2012)); *see also* David W. Opderbeck, *Does the Communications Act of 1934 Contain A Hidden Internet Kill Switch?*, 65 FED. COMM. L.J. 1 (2013). Others opine that the United States does not have an internet kill switch, although Congress attempted to legislate such a kill switch in the past. *See, e.g.*, Cybersecurity Act of 2009, S. 773, 111th Cong. § 18(2) (2009) (proposing to empower the President to "declare a cybersecurity emergency and order the limitation or shutdown of Internet traffic to and from any compromised Federal

B. PLURALITY OF (STATE) ACTORS

As the state considers its possible courses of action in promoting its goals in cyber activities, perhaps the first question it must answer is whether to act in its capacity as the executive (which is akin, in that respect, to a superuser with legal authorization to act) or as a regulator (by invoking the legal powers to collect information, analyze it, form policies, issue norms, enforce these norms, and assess impact). While this Article will further argue in Section III.B that the state can affect behavior through its role as a superuser by using its power to influence the market, consumers, and other states, the focus here is on cyber regulation performed by the state when acting as *a regulator*.

Yet regulation itself is not a single process or outcome; rather, it is best understood as polycentric or plural.[59] Regulators must often consider more than one form of regulation to find the optimal blend between direct and indirect strategies. In modern commerce, there is no legal void. One form or another of direct or indirect regulation is likely present at any given social sphere.[60] Moreover, there is hardly ever just a single regulator present. The structure of the modern regulatory state contains an inherent tension between horizontal regulators, which concern themselves with the greater market (for example, those in charge of antitrust or those in charge of labor and employment across sectors), and sector-specific (vertical or silo) regulators, which are in charge of just one segment of the public service (such as health, agriculture, or finance).[61] Such silos themselves may generate friction zones. For instance, regulating the production of livestock usually involves not only the regulator of agriculture, but also the regulator of veterinary services, waters,

---

government or United States critical infrastructure information system or network"); The Protecting Cyberspace as a National Asset Act, S. 3480, 111th Cong. § 249 (2010) (proposing to grant the President the power to declare a "national cyber emergency" and disable the internet in the event of an "emergency"). *Cf.* Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. § 2(c) (2011) (including a provision that "neither the President . . . or [sic] any officer or employee of the United States Government shall have the authority to shut down the Internet").

59. For more on this topic, see generally Julia Black, *Constructing and contesting legitimacy and accountability in polycentric regulatory regimes*, 2 REGULATION & GOVERNANCE 137 (2008).

60. As previously discussed, Lawrence Lessig views regulation of behavior as a non-binary mixture between four modalities: law, market, social norms and architecture. *See* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 513 (1999). He argues there is always a mix of direct and indirect strategies, and that the regulator needs to find the optimal mixture. *See id.*

61. For a general discussion on the horizontal and vertical agencies in a supra-national context, see generally Pierre Larouche, *Coordination of European and Member State Regulatory Policy: Horizontal, Vertical and Transversal Aspects*, *in* REGULATION THROUGH AGENCIES IN THE EU: A NEW PARADIGM OF EUROPEAN GOVERNANCE 164–79 (Damien Geradin, Rodolphe Muñoz & Nicolas Petit eds. 2006).

or health. Such frictions may be productive as a form of checks and balances on the regulatory power, but they may also prove disruptive.[62]

Cyber regulation is hardly unique in this regulatory sense. It is well known that many governmental entities partake in cyber regulation. The fact that there are various types of regulators to regulate different aspects of a certain field is therefore not surprising. This Section will provide a snapshot of the various governmental bodies involved in cyber regulation as these lines are written. This exercise is important because it captures the institutional complexities as they exist in 2019,[63] and thereby provides the necessary groundwork for understanding the challenges the state faces in addressing its regulatory functions regarding offense, defense, and surveillance. This snapshot further suggests that cyber regulation presents a test case of how a plurality of regulators could lead to suboptimal results if regulation is left uncoordinated.

In order to demarcate the boundaries of this investigation, it would be helpful to first get a better sense of what forms of regulation should be considered as "cyber" regulation. Generally, "cyber" should include any regulation of a D2D activity that refers to offense, defense, and surveillance.[64] But the variety of activities that could relate to these elements is vast. In that context, several qualifications may be in order. First, cyber regulation would include the regulation of networks, mainly the internet. Here, it is necessary to distinguish between different forms of regulations over the internet, as not every internet-related regulation will be deemed "cyber regulation" (or at least not a direct one). For example, regulation of online copyright infringement, or domain names, are not "cyber" under this Article's suggested taxonomy. Second is information security regulation. Such regulation could refer not only to the internet, but also to anyone who retains information. Third is regulation of cyber-related commerce—for example, regulation of the use, development, and import or export of technology, whether software or hardware, which plays part in cyber offense, defense, or surveillance.

A potential starting point of the analysis is identifying the basic goals of cyber regulation. Let us assume that these goals are defending against cybercrimes (promoting personal safety and national security) and generating economic growth (in the form of intellectual property or otherwise). Under

62. *See generally* Shmueli et al., *supra* note 7.

63. In writing this Section, we are well aware that in the future the institutional design may, and in fact is likely to, change. But providing a description of how things stand, institutionally, in 2019 is important if we want to understand the contemporary challenges. Moreover, precisely because institutional designs change, the description provided here will be useful for any future research on the historical evolution of cyber governance.

64. *See supra* note 3.

this premise, promoting innovation is instrumental to both. As with respect to any regulation, cyber regulation operates within a certain constitutional structure, the goals of which are maintaining a certain institutional design of separation of powers and protecting fundamental rights. From these stylized starting points, it is not difficult to surmise that cyber regulation can hardly be performed by a single regulator if it desires optimal levels of security. The complexities of the technology, economic incentives, multiplicity of networks in any given social domain, and deep enmeshment with privately owned industry suggests that one should not be surprised to find a network of state and private (or co-regulators) addressing technological networks.[65] Furthermore, "cyber" is not confined to the state. It is a transnational and international matter, which might also require international intervention, possibly through regulatory mechanisms.[66] Thus, the state could regulate cyber both domestically and transnationally to the extent that the state establishes jurisdiction over a segment of the network, or to the extent that it joins forces with other jurisdictions that do.

Once again, this is hardly new. The challenge is to minimize the negative features of polycentric regulation by reducing disruptive frictions (or overlaps) on one hand and regulatory gaps on the other. This Article uses the United States as an example of the plurality of governing bodies in cyber to demonstrate such sub-optimality. As a general matter, almost any governmental body could affect cyber regulation, either by being present in the networked dimension or by issuing rules and guidelines that pertain to interacting with it in this dimension. Any agency with some sort of internet presence could be vulnerable to cyberattacks,[67] which raises potential regulatory concerns. To name but a few examples, public government information may be manipulated, services may be disrupted, or data pertaining to the government or to individuals who interact with the government may be accessible to unauthorized entities. To the extent that a public body governs its own cybersecurity, it can be seen as performing self-regulation. This may

65. For more on private and co-regulators in the cyber context, see generally TATIANA TROPINA & CORMAC CALLANAN, SELF- AND CO-REGULATION IN CYBERCRIME, CYBERSECURITY AND NATIONAL SECURITY (2015).

66. See, for instance, how under the U.S. National Cyber Strategy, one of the objectives is to "encourage universal adherence to cyber norms." *The National Cyber Strategy of the United States of America*, THE WHITE HOUSE 20 (Sept. 2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. *Cf.* Deeks, *supra* note 20.

67. *See* Gus P. Coldebella & Brian M. White, *Foundational Questions Regarding the Federal Role in Cybersecurity*, 4 J. NAT'L SECURITY L. & POL'Y 233, 239 (2010) (listing the IRS and the Department of Health and Human Services as examples of agencies which have an internet presence vulnerable to exploitation).

raise issues of accountability to the extent that such self-regulation may authorize the infringements of rights or other public interests, for example, in the course of authorizing countermeasures or in deciding to forgo certain defensive lines, thereby allowing access to certain information. It may also raise potential concerns relating to the relative expertise of each government body, as well as to the overall integrity and coherence of the measures involved.

But the scope here, as stated, is distinct. We seek to understand which government bodies within the executive govern cyber regulation outside their own protective domain. First, and perhaps foremost, is the White House, led by the U.S. president.[68] The White House regulates cyber in various capacities. To begin, under the U.S. regime, the President is the Commander in Chief of the armed forces.[69] Under his authority, the President can set regulations by issuing executive orders (EOs).[70] Indeed, many U.S. presidents have signed EOs related to cybersecurity, mostly regarding the protection of critical infrastructures and key assets from cyberattacks.[71] The President also signs

68. Mainly, it includes the President, the Vice President, the Executive Office of the President (EOP), and the Cabinet. *See The Executive Branch*, THE WHITE HOUSE https://www.whitehouse.gov/1600/executive-branch (last visited July 20, 2019).

69. Under Article II of the Constitution, the President is the Commander-in-Chief and is empowered "to conduct warrantless surveillance of enemy forces for intelligence purposes to detect and disrupt armed attacks on the United States." Alberto Gonzales, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President of the United States* 1 (Jan. 19, 2006), http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB178/surv39.pdf. Alternately, Congress authorized the President "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001 . . . ." Authorization for Use of Military Force, S.J. Res. 23, 107th Cong. § 2(a) (Sept. 18, 2001).

70. While there are no constitutional provisions or statutes that explicitly permit EOs, it is beyond the scope of this Article to discuss their sources or legality. For more on executive orders, see generally Erica Newland, *Executive Orders in Court*, 124 YALE L.J. 2026 (2015).

71. The first cyber-related EO was issued by President Ronald Reagan in 1981. *See* Exec. Order No. 12333, 40 Fed. Reg. 235 (December 4, 1981). This was further amended over time by Executive Order No. 13284, 68 Fed. Reg. 4057 (Jan. 23, 2003), Executive Order No. 13355, 69 Fed. Reg. 53593 (Aug. 27, 2004), and Executive Order No. 13470, 73 Fed. Reg. 45325 (July 30, 2008)). EO No. 12333 authorized the Attorney General to approve the use of any technique for intelligence purposes within the United States or against a U.S. person abroad. *See* Liu, *supra* note 41*,* at 3. In February 2015, President Barak Obama signed an EO that urged companies to share cybersecurity-threat information with the federal government and other companies. *See* Katie Zezima, *Obama Signs Executive Order on Sharing Cybersecurity Threat Information*, THE WASH. POST (Feb. 12, 2015), http://www.washingtonpost.com/blogs/post-politics/wp/2015/02/12/obama-to-sign-executive-order-on-cybersecurity-threats/?tid=sm_tw. One of the latest cyber-related EOs was issued on May 11, 2017. *See* Exec. Order No. 13800, 82 Fed. Reg. 32172 (May 11, 2017). EO No. 13800 Focuses primarily on the cybersecurity of federal networks, critical infrastructure, and the United States more generally. *See generally id.* It mandates federal agencies to comply with the NIST Cybersecurity Framework

executive agreements and treaties. Such agreements and treaties could relate to cyber activities both directly and indirectly. Short of a binding regulation, the President may also issue guidelines for federal departments and agencies, industries, and consumers on how to strengthen cybersecurity.[72] The President is also in charge of the Office of the Director of National Intelligence (ODNI), the director of which is the head of the U.S. Intelligence Community.[73] Within ODNI, "[t]he National Intelligence Manager for Cyber is charged with integrating cyber intelligence within the US Government and of looking strategically for ways to improve the quantity, quality, and impact of cyber intelligence."[74] Moreover, ODNI has recently created the Cyber Threat Framework designed "to enable consistent characterization and categorization of cyber threat events, and to identify trends or changes in the activities of cyber adversaries."[75] Finally, the President also possesses the ability to veto bills passed by Congress and thereby influences cyber-related legislation.[76]

The regulatory complex in the White House also consists of the Executive Office of the President (EOP) and the White House Office.[77] The EOP and the White House Office oversee several cyber-related agencies, *inter alia*, the National Security Council (NSC), Homeland Security Council, President's Intelligence Advisory Board, and Office of Science and Technology Policy.[78] The EOP also houses the U.S. Digital Service, a technology unit that provides consultation services to federal agencies on information technology.[79] Of special importance is the Office of Management and Budget (OMB),[80] which

---

and requires the assessment of risk, development of an action plan, and development of policy regarding critical infrastructure. *See id.* It also provides guidance on employee training and education on cybersecurity. *See id.*; *Executive Order 13800: Strengthening Cybersecurity of Federal Networks and Critical Infrastructure*, OBSERVEIT (May 27, 2017), https://www.observeit.com/blog/executive-order-13800.

72. *See The National Cyber Strategy*, *supra* note 66.

73. *See Who We Are*, DNI, https://www.dni.gov/index.php/who-we-are (last visited July 20, 2019).

74. *See Building Blocks of Cyber Intelligence*, DNI, https://www.dni.gov/index.php/cyber-threat-framework (last visited July 20, 2019).

75. *Id.*

76. Congress, however, may also override a veto by a two-thirds vote in both the Senate and the House of Representatives. *See* U.S. CONST. art. I, § 7, cl. 2.

77. *Executive Office of the President*, THE WHITE HOUSE https://www.whitehouse.gov/administration/eop (last visited July 20, 2019).

78. *Id.*

79. *See Our Mission*, USDS, https://www.usds.gov/mission (last visited July 20, 2019).

80. The Federal Information Security Modernization Act of 2014 requires OMB to "oversee[] and monitor[] agencies' implementation of security requirements; . . . operate the federal information security incident center; and . . . provide agencies with operational and technical assistance, such as that for continuously diagnosing and mitigating cyber threats and vulnerabilities." GOVERNMENT ACCOUNTABILITY OFFICE, HIGH RISK SERIES: AN UPDATE

is relevant to the regulatory process in general, primarily via the Office of Information and Regulatory Affairs (OIRA).[81] The latter conducts regulatory impact assessments for regulatory proposals proposed by agencies subject to such review. This assessment primarily focuses on coordination with other agencies and cost-benefit assessment. In the cyber context, OMB recently issued the Federal Cybersecurity Risk Determination Report and Action Plan, which provides an assessment of government cybersecurity risks, identifies actions to improve cybersecurity at the federal level, and acknowledges that "agencies must work together over the coming months to identify how to implement those actions."[82]

Second, beyond the White House, the various offices and departments at the executive level could all potentially regulate cyber.[83] This regulation may (likely) generate a plurality of less-than-coherent set of policies and measures, not only because each of the offices comes to the table with a different mission and perspective,[84] but also because the regulatory agencies are not fully aligned under the White House. Some federal agencies are subject to OMB, while others are independent federal agencies. The agencies operating under the White House—the Department of Homeland Security (DHS), Department of

237 (2015), https://www.gao.gov/assets/670/668414.txt (last visited July 31, 2019). OMB is also tasked "to annually assess agencies' implementation of data breach notification policies and procedures[] and specifies that the agency head ensure all personnel are held accountable for complying with information security." *Id.*; *see also* The 2014 Federal Information Security Modernization Act 2014, Pub. L. No. 113–283, 128 Stat. 3073 (2014); *High Risk List*, GAO, http://www.gao.gov/highrisk/protecting_the_federal_government_information_systems/why_did_study#t=1 (last visited July 20, 2019).

81. OIRA has attracted considerable scholarly attention, an example of which is the debate between Lisa Heinzerling, *Inside EPA: A Former Insider's Reflections on the Relationship Between the Obama EPA and the Obama White House*, 31 PACE ENVTL. L. REV. 325 (2014) and Cuss Sunstein, *The Office of Information and Regulatory Affairs: Myths and Realities*, 126 HARV. L. REV. 1838 (2013).

82. *Federal Cybersecurity Risk Determination Report and Action Plan*, OMB 2 (May 2018), https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf.

83. Relevant agencies include: the Cabinet, Department of Agriculture, Department of Commerce, Department of Defense, Department of Education, Department of Energy, Department of Health and Human Services, Department of Homeland Security, Department of Housing and Urban Development, Department of the Interior, Department of Justice, Department of Labor, Department of State, Department of Transportation, Department of the Treasury, and Department of Veterans Affairs. For an overview of each office/department, see *The Executive Branch*, *supra* note 68.

84. Naturally, the notion that different agencies sometimes overlap is not uncommon and existed much prior to the emergence of cyber. For example, the goals of an environmental protection agency could clash with the department of energy. However, as we further show, we argue that such diversity in cyber is vast.

Commerce (DOC), Department of Defense (DOD), Department of Energy (DOE), Department of Health and Human Services (DHHS), Department of Justice (DOJ), Department of Transportation (DOT), Department of the Treasury (DoT), and the Department of State (DOS)—each have a distinct concern with respect to cyber.

Within this group, DHS plays a particularly important role. It is responsible for securing the ".gov" domain as well as deploying and running the National Cyber Protection System (commonly referred to as Einstein 1, 2, and 3).[85] DHS runs many agencies, centers, and programs, currently led by its Cybersecurity and Infrastructure Security Agency (CISA).[86] It is comprised of a Cybersecurity Division, Infrastructure Security Division (including the Infrastructure Information Collection Division (IICD), Infrastructure Security Compliance Division, and National Infrastructure Coordinating Center), National Risk Management Center, Emergency Communications Division, and Protective Security Coordination Division.[87] CISA also includes the National Cybersecurity and Communications Integration Center, which integrates a Computer Emergency Readiness Team (CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).[88]

DOC runs the National Institute of Standards and Technology (NIST), which serves as an agency within DOC. While considered a non-regulatory agency, NIST develops recommended cybersecurity frameworks for the government, which consist of standards, guidelines, and best practices.[89] In

85. *See* Michael Chertoff, *Foreword to Cybersecurity Symposium: National Leadership, Individual Responsibility*, 4 J. NAT'L SECURITY L. & POL'Y 1, 4 (2010).

86. The Cybersecurity and Infrastructure Security Agency (CISA) acts as "the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future." *About CISA*, U.S. DEP'T OF HOMELAND SEC., https://www.dhs.gov/cisa/about-cisa (last visited July 20, 2019). It is tasked to provide "extensive cybersecurity and infrastructure security knowledge and practices to its stakeholders, shares that knowledge to enable better risk management, and puts it into practice to protect the Nation's essential resources." *Id.* Prior to the enactment of the Cybersecurity and Infrastructure Security Agency Act of 2018, this task was appointed to the National Protection and Programs Directorate (NPPD), a program established in 2007 within the DHS. *See* Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115–278, 132 *Stat.* 4168 (2018).

87. *See* Cybersecurity & Infrastructure Security Agency*, Organization Chart*, U.S. DEP'T OF HOMELAND SEC., https://www.cisa.gov/sites/default/files/publications/CISA_101_org_chart_082020_508.pdf.

88. *See About CISA*, *supra* note 86.

89. Regarding cybersecurity, NIST facilitates and supports the development of voluntary industry-led standards and practices to reduce cyber risks to critical infrastructure. *See* Cybersecurity Enhancement Act of 2014, Pub. L. No. 113–274, § 101(b), 128 Stat. 2971 (2014).

August 2017, NIST published its National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, which should aid organizations in, *inter alia*, planning, implementing, and monitoring a successful cybersecurity program.[90] DOC also runs agencies such as the National Telecommunications and Information Administration, which advises the President on, *inter alia*, telecommunications and information policy issues, including cyber.[91]

DOD is responsible for defending its own networks, systems, and information;[92] conducting "cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict";[93] "defend[ing] forward[94] to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict";[95] and "strengthen[ing] the security and resilience of networks and systems that contribute to . . . U.S. military advantages."[96] DOD also operates agencies like

90. *See* William Newhouse, Stephanie Keith, Benjamin Scribner & Greg Witte, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, NIST SPECIAL PUBLICATION 800–181, 7 (Aug. 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800–181.pdf?trackDocs=NIST.SP.800–181.pdf (further revised in November 2020).

91. *See About NTIA*, U.S. DEPT. OF COM., http://www.ntia.doc.gov/about (last visited July 20, 2019).

92. Since 2009, the U.S. Strategic Command (STRATCOM) monitors attacks on DOD systems and is responsible, *inter alia*, for securing the ".mil" domain. *See* COMM. ON OFFENSIVE INFO. WARFARE, NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 35 (William A. Owens et al. eds., 2009) [hereinafter: COMM. ON OFFENSIVE].

93. *Department of Defense Cyber Strategy (summary) 2018*, U.S. DEP'T OF DEF., https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/cyber_strategy_summary_final.pdf.

94. There is no agreed upon definition of what "defend forward" means within the Defense Cyber Strategy summary. Some suspect that it refers to conducting activities outside of U.S. networks and that it entails "operations that are intended to have a disruptive or even destructive effect on an external network . . . ." Robert Chesney, *The 2018 DOD Cyber Strategy: Understanding 'Defense Forward' in Light of the NDAA and PPD-20 Changes*, LAWFARE (Sept. 25, 2018), https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes.

95. *Department of Defense Cyber Strategy (summary) 2018*, U.S. DEP'T OF DEF. (Sept. 18, 2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/cyber_strategy_summary_final.pdf.

96. *See Department of Defense Cyber Strategy (summary) 2018*, U.S. DEP'T OF DEF. 1 (Sept. 18, 2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/cyber_strategy_summary_final.pdf. Notably, while the 2018 strategy was only published in a summary version, the DOD published a full strategy in 2015, which is no longer in force. Back in 2015, the DOD was responsible, *inter alia*, for defending the U.S. homeland and U.S. national interests against cyberattacks of "significant consequence" and providing cyber support to military operational and contingency plans. The Department of Defense Cyber Strategy, U.S.

the National Security Agency (NSA). As was revealed by Edward Snowden, the NSA also collects a considerable amount of data, which it then analyzes as part of its intelligence mission.[97] Some of these activities are conducted in the NSA's capacity as an operational agency and a superuser; the NSA obtains data with or without permission from the companies that generate, hold, or manage this data, seemingly outside the effective reach of the judicial process.[98] As the current debate regarding the applicability of constraints on the collection of information on U.S. persons[99] versus non-U.S. persons[100] reveals, it appears

---

DEP'T OF DEF. 3 (Apr. 2015), https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf.

97. *See* Glenn Greenwald, *NSA Prism Program Taps into User Data of Apple, Google and Others*, THE GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data?guni=Article:in%20body%20link.

98. As revealed by the Washington Post, under two programs ("PRISM" and upstream collection), the NSA and the FBI were allowed direct access to servers of leading internet companies. Barton Gellman & Laura Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, WASH. POST (June 6, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html. Under this form of partnership, companies did not directly provide information, but rather equipped the NSA with the proper tools to directly tap into their central servers via either "backdoors" (i.e., intentional flaws in a cryptographic algorithm or implementation allowing bypassing of security mechanisms) or allowing upstream collection. *Id.* Another form of public-private partnership was revealed in 2006, within an Electronic Frontier Foundation (EFF) class action lawsuit against AT&T. Mark Klein, a former AT&T technician, reported in his statement that AT&T (located in San Francisco) uses a "splitter" device, which makes a complete copy of the internet traffic that AT&T receives, and diverts it onto a separate fiber optic cable, which is connected to a room controlled by the NSA. *Wiretap Whistle-Blower's Account: Statement of Mark Klein*, WIRED (Apr. 6, 2006), http://archive.wired.com/science/discoveries/news/2006/04/70621.

99. The Foreign Intelligence Surveillance Act (FISA) regulated all electronic surveillance of American citizens or permanent residents within the United States for foreign intelligence or international counterterrorism purposes. *See* 50 U.S.C. § 1805 (2012). Under FISA, the Foreign Intelligence Surveillance Court (FISC) was formed. *See* Sinha, *supra* note 41, at 874. FISC is a "secret court," comprised of federal district judges that examine classified information in a closed, *ex-parte* hearing. *Id.* (internal notations omitted). Warrants are authorized in the existence of a "probable cause to believe that the target of surveillance is an agent of a foreign state or a terrorist group." *Id.* (internal citations omitted).

100. The NSA conducts at least two prime interior methods of cyber intelligence to combat national security threats: metadata collection and gathering electronic communications through the "PRISM" program and upstream collection. The first, metadata collection, is conducted pursuant to Section 215 of the USA Patriot Act, 50 U.S.C. § 1861 (2012). Under Section 215, the director of the FBI or a designee of the Director (like the NSA) can apply for a FISC order requiring the production of "any tangible things" (e.g., records held by a telecommunications provider) if there are "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation" into foreign intelligence, international terrorism, or espionage. 50 U.S.C. § 1861(a)(1), (a)(2)(B) (2012). Under the

that a new equilibrium[101] regarding what constitutes surveillance is in the making.[102] Finally, the U.S. Cyber Command (CYBERCOM) is charged with "direct[ing], synchroniz[ing], and coordinat[ing] cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners."[103]

DOE engages in cybersecurity that relates to energy. Mostly, its goal is to enhance the security and reliability of the nation's electric grid. Administrated by the Office of Electricity Delivery and Energy Reliability (OE), DOE published Cybersecurity Strategy, partially handled by the Office of Cybersecurity, Energy Security, and Emergency Response.[104] This strategy comprises several factors and includes, *inter alia*, adopting standard operating procedures for DOE cybersecurity incident reporting and response and increasing enterprise-wide sharing of analytics and real-time threat information in order to improve enterprise-wide cybersecurity situational awareness, incident detection, and tactical response.[105]

At first glance, DHHS does not appear to be a cyber regulator. But due to the importance of sensitive information and the reliance on health services,

---

second method, gathering electronic communications, the NSA gathers electronic communications, including content, of overseas, foreign targets whose communications flow through American networks. Under PRISM, the NSA taps directly into the central servers of U.S. internet companies, extracting audio and video chats, photographs, e-mails, documents, and connection logs of non-U.S. targets. *See supra* note 98. The NSA also uses upstream collection, which is the gathering of electronic communications, including metadata and content, of foreign targets overseas whose communications flow through American networks. The PRISM program and upstream collection are conducted pursuant to Section 702 of the Foreign Intelligence Surveillance Act (FISA), added by both the FISA Amendments Act of 2008 (FAA) and EO No. 12333. *See* JOHN W. ROLLINS & EDWARD C. LIU, CONG. RSCH. SERV., R43134, NSA SURVEILLANCE LEAKS: BACKGROUND AND ISSUES FOR CONGRESS (2013); Gellman & Poitra, *supra* note 98.

101. For an argument on how "the Supreme Court adjusts the scope of [constitutional protection] in response to new facts in order to restore the status quo level of protection," see Kerr, *supra* note 18.

102. For more on surveillance in the post-Snowden revelations, see generally Elkin-Koren & Haber, *supra* note 42. The NSA practices also led—or at least pushed—the European Union to strengthen the protection of personal data through, *inter alia*, its General Data Protection Regulation and the Privacy Shield, an E.U.-U.S. treaty signed in 2016. *See generally* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115 (2017).

103. *Mission*, U.S. CYBER COMMAND, https://www.cybercom.mil/About/Mission-and-Vision (last visited July 20, 2019).

104. *See* CYBERSECURITY STRATEGY, U.S. DEP'T OF ENERGY (2018), https://www.energy.gov/sites/prod/files/2018/07/f53/EXEC-2018-003700%20DOE%20Cybersecurity%20Strategy%202018-2020-Final-FINAL-c2.pdf; *About Us*, ENERGY.GOV, https://www.energy.gov/ceser/about-us (last visited July 20, 2019).

105. *See* CYBERSECURITY STRATEGY, *supra* note 104, at 5–7.

this executive department also regulates important cyber-related activities. DHHS has "the authority to promulgate and enforce regulations regarding information security measures [for] healthcare entities and their associates . . . ."[106] Such information would usually contain data on "patients, research subjects, and individuals whose medical information they collect/maintain."[107] More closely, in terms of cyber-regulation, the health care industry formed a Cybersecurity Task Force, which issued a report to Congress in 2017, calling for, *inter alia*, "a collaborative public and private sector effort to protect our healthcare systems and patients from cyber threats."[108]

DOJ's role in cyber regulation, while not necessarily obvious, is highly important. DOJ's National Security Division (NSD) is tasked with combatting terrorism and other threats to national security, including cyber threats.[109] DOJ's Cybersecurity Unit, within the Computer Crime and Intellectual Property Section (CCIPS), serves as a gatekeeper by examining government activities in cyber and aids in shaping cybersecurity legislation.[110] Generally, the CCIPS is responsible for administering strategies in combating computer crimes.[111]

While, generally speaking, the DOJ provides recommendations for legislation and plays a key role in guiding U.S. officials in exercising their legal powers, its role in shaping cyber regulation is a unique one. The Office of the U.S. Attorneys, which fall under the DOJ, make decisions on which incidents to investigate and prosecute. Those decisions are highly important for shaping the cyber realm not merely domestically, but also internationally (if and when the Office decides to participate in international efforts to combat cyber-related incidents). DOJ coordinates national security cyber threat efforts through a nationwide network of National Security Cyber Specialists ("NSCS network").[112] In addition, DOJ parents enforcement agencies within the

106. David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287, 296 (2014).

107. *Id.*; *see also* 42 U.S.C. § 1320d–2(d)(1) (2012).

108. HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE, PUB. HEALTH EMERGENCY, https://www.phe.gov/Preparedness/planning/CyberTF/Pages/default.aspx (last visited July 20, 2019).

109. *See About the Division*, U.S. DEP'T OF JUSTICE, http://www.justice.gov/nsd/about-division (last visited July 20, 2019).

110. *See Cybersecurity Unit*, U.S. DEP'T OF JUSTICE, http://www.justice.gov/criminal-ccips/cybersecurity-unit (last visited July 20, 2019).

111. *See The Computer Crime and Intellectual Property Section (CCIPS)*, U.S. DEP'T OF JUSTICE, http://www.justice.gov/criminal-ccips (last visited July 20, 2019).

112. *See Cyber Threats: Law Enforcement and Private Sector Responses: Hearing Before the Subcomm. on Crime and Terrorism Comm. on Judiciary U.S. Senate*, 113th Cong. 6 (2013) (statement of Jenny

executive that also regulate behavior, as will be further detailed in the following paragraphs. For example, the Federal Bureau of Investigation (FBI) is responsible for law enforcement and counterintelligence.[113] As for investigations,[114] the FBI, *inter alia*, issues national security letters, which are secret subpoenas evading judicial oversight.[115]

The Transportation Security Administration (TSA), as a division within DHS, has the authority to regulate cybersecurity in the transportation sector. Among other things, TSA monitors oil and gas pipelines' cybersecurity and issues security guidelines related to pipelines that are operated by computerized Supervisory Control and Data Acquisition (SCADA) systems and are therefore vulnerable to cyberattacks.[116]

The DOT directs and coordinates policies on cybersecurity issues that could harm transportation safety.[117] Mainly, DOT collaborates with DHS to ensure the safety of pipelines controlled by SCADA systems.[118] DOT is also in charge of securing transportation systems and "secur[ing] operation of motor vehicles equipped with advanced electronic control systems."[119] Not to

---

A. Durkan, U.S. Attorney, W.D. Wash., Dep't of Justice), https://www.judiciary.senate.gov/imo/media/doc/5-8-13DurkanTestimony.pdf.

113. *See* COMM. ON OFFENSIVE, *supra* note 92, at 291.

114. Cyber operations in the FBI are commenced mainly under the National Security Branch (NSB) and the FBI Cyber Division, which includes "cyber based terrorism, espionage, computer intrusions, and major cyber fraud." *Cyber Resources*, Domestic Security Alliance Council, https://www.dsac.gov/topics/cyber-resources (last visited Mar. 21, 2021). It includes various initiatives and partnerships, e.g., The Internet Crime Complaint Center; The National Cyber Investigative Joint Task Force; Cyber Task Forces; iGuardian; eGuardian; InfraGard: Protecting Infrastructure; National Cyber-Forensics & Training Alliance; and Cyber Action Team. *See Testimony*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/news/testimony/the-fbis-cyber-division (last visited July 20, 2019); *Cyber Crime*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/about-us/investigate/cyber (last visited July 20, 2019).

115. The FBI is authorized to seek non-content information that is relevant to an authorized national security investigation. *See generally* 18 U.S.C. § 2709 (2012); 15 U.S.C. §§ 1681u–1681v (2012); 12 U.S.C. § 3414 (2012).

116. *See, e.g.*, TRANSP. SEC. ADMIN., PIPELINE SECURITY GUIDELINES (2011).

117. More specifically, DOT plans to "[d]evelop modal cyber threat models for transportation critical infrastructure to enhance integrated cybersecurity and safety research priorities." *Strategic Plan for FY 2018–2022*, DTIC, at 8 (Feb. 2018), https://www.transportation.gov/sites/dot.gov/files/docs/mission/administrations/office-policy/304866/dot-strategic-plan-fy2018-2022.pdf.

118. *See Mission & Goals*, PIPELINE AND HAZARDOUS MATERIAL SAFETY ADMIN., http://www.phmsa.dot.gov/about/mission (last visited July 20, 2019).

119. This is done by the National Highway Traffic Safety Administration (NHTSA). *See generally* NAT. HIGHWAY TRAFFIC SAFETY ADMIN., DOT HS 812 075, A SUMMARY OF CYBERSECURITY BEST PRACTICES (2014), http://www.nhtsa.gov/DOT/NHTSA

be confused with DOT, the Department of the Treasury (DoT) is responsible for securing its own network. But much like any other agency, it regulates sectorial industries that could be subject to all three cyber components, although it mainly focuses on defense. Banks are a good example. They are regulated federally by the Office of the Comptroller of the Currency, which is an independent bureau within DoT.[120]

DoS is responsible for coordinating international efforts to improve cybersecurity. This mission includes:

> coordinating the Department's global diplomatic engagement on cyber issues; serving as the Department's liaison to the White House and federal departments and agencies on those matters; advising the Secretary and Deputy Secretaries on cyber issues and engagements; acting as liaison to public and private sector entities on cyber issues; and coordinating the work of regional and functional bureaus within the Department engaged in these areas.[121]

More specifically, the mission of the Office of the Coordinator for Cyber Issues ("S/CCI") is "to promote [in partnership with other countries] an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation."[122]

As noted, the executive complex also includes the independent agencies, which play a crucial role in cyber regulation. These agencies issue rules and guidelines, enforce regulation, and actively engage in several committees empowered to shape cyber regulation.[123] More specifically, the Federal Communications Commission (FCC) regulates communications by radio, television, wire, satellite, and cable. As such, it serves as the primary authority

---

/NVS/Crash%20Avoidance/Technical%20Publications/2014/812075_CybersecurityBestPractices.pdf.

120. The OCC "regulates . . . all national banks and federal savings associations as well as federal branches and agencies of foreign banks." *About the OCC*, http://www.occ.gov/about/what-we-do/mission/index-about.html (last visited July 20, 2019).

121. MELISSA HATHAWAY, UNITED STATES OF AMERICA CYBER READINESS AT A GLANCE 21 (2016), https://potomacinstitute.org/images/CRI/CRI_US_Profile_Web.pdf.

122. *Office of the Coordinator for Cyber Issues: Our Mission*, U.S. DEP'T OF STATE, https://www.state.gov/bureaus-offices/bureaus-and-offices-reporting-directly-to-the-secretary/office-of-the-coordinator-for-cyber-issues/ (last visited Jan. 5, 2021). Between 2009 and 2017, the mission was defined as: "coordination function spans the full spectrum of cyber-related issues to include security, economic issues, freedom of expression, and free flow of information on the Internet." *Office of the Coordinator for Cyber Issues*, U.S. DEP'T OF STATE, https://2009-2017.state.gov/s/cyberissues//index.htm (last visited July 20, 2019).

123. *See, e.g.*, *CNSS Responsibilities*, COMM. ON NAT. SECURITY SYS. (CNSS), https://www.cnss.gov/CNSS/about/about.cfm (last visited July 20, 2019).

for regulating communication technologies. Among its duties, the FCC issues licenses, regulates common carriers, and enforces such regulations.[124] Also within the realm of infrastructure, the Federal Energy Regulatory Commission (FERC) is tasked with protecting the electric utility industry in the United States. FERC sets and enforces security standards.[125] Moving to a different type of infrastructure, The Federal Reserve Board of Governors governs the Federal Reserve System and the U.S. central bank. It regulates private banking institutions and provides financial services to the U.S. government, public, and financial institutions.[126] As the banking system is fully networked—and as the financial technology sector emerges as a key component of the structure of the modern economy—cyber defense, attack, and surveillance in this domain are crucial. Also within the financial sector, the Federal Trade Commission (FTC) enforces federal antitrust and consumer protection laws. In the cyber sense, the FTC regulates companies by shaping business practices and information sharing,[127] and by promulgating and "enforc[ing] regulations regarding information security measures financial institutions . . . employ[ed] to protect [personal,] sensitive information . . . ."[128] Beyond these agencies, in 2017, President Trump signed an Executive Order which established the American Technology Council (ATC), set "to promote the secure, efficient, and economical use of information technology" by transforming and modernizing the delivery of digital services and federal information technology.[129]

---

124. *See What We Do*, FED. COMS. COMM'N, https://www.fcc.gov/what-we-do (last visited July 20, 2019).

125. *See What FERC Does*, FED. ENERGY REGULATORY COMM'N, http://www.ferc.gov/about/ferc-does.aspx [https://perma.cc/F4WQ-GS56] (last visited July 20, 2019). For further information on cyber security and the FERC, see generally Susan J. Court, *Federal Cyber-Security Law and Policy: The Role of the Federal Energy Regulatory Commission*, 41 N. KY. L. REV. 437 (2014) (detailing the role of the Federal Energy Regulatory Commission).

126. *See About the Fed*, Bd. Of Governors of the FED. RESERVE SYS., http://www.federalreserve.gov/aboutthefed/mission.htm (last visited July 20, 2019).

127. *See* 15 U.S.C. § 45(a) (2012); *About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc (last visited July 20, 2019).

128. Thaw, *supra* note 107, at 296. This is as set under the Gramm-Leach-Bliley Act. *See* Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106–102, 113 Stat. 1338 (1999).

129. The ATC is tasked to "(i) coordinate the vision, strategy, and direction for the Federal Government's use of information technology and the delivery of services through information technology; (ii) coordinate advice to the President related to policy decisions and processes regarding the Federal Government's use of information technology and the delivery of services through information technology; and (iii) work to ensure that these decisions and processes are consistent with the policy set forth in section 1 of this order and that the policy is being effectively implemented." Exec. Order No. 13794, 82 Fed. Reg. 20811, § 1 (Apr. 28,

Finally, the partial list of agencies referred to above would be even more incomplete at the federal level if it did not include the Central Intelligence Agency (CIA) and the armed forces. The CIA gathers intelligence, provides national security assessments to policymakers, and is deeply engaged in cyber operations.[130] As a general matter,[131] it serves as the sole agency responsible for conducting "special activities."[132] This agency is an operator or an actor more than a regulator, and, in that respect, it falls into a different category.

Similarly, the military is a direct actor rather than a classic regulator. Its Commander in Chief, the President, may perform regulatory functions regarding the way the military carries out its mission, as does the DOD (via the Secretary of Defense) to an extent. However, we should be careful before we ascribe to the military itself, or to the CIA for that matter, any direct regulatory functions. The military engages in cyberwarfare; more specifically, the U.S. Army Cyber Command (ARCYBER), a component command of USCYBERCOM, integrates and conducts cyberspace operations, electronic warfare, and information operations.[133] Naturally, the U.S. Army Intelligence

2017). It is comprised of the President (as Chairperson); Vice President; Secretary of Defense; Secretary of Commerce; Secretary of Homeland Security; Director of National Intelligence; Director of the Office of Management and Budget (OMB); Director of the Office of Science and Technology Policy; U.S. Chief Technology Officer; Administrator of General Services; Senior Advisor to the President; Assistant to the President for Intragovernmental and Technology Initiatives; Assistant to the President for Strategic Initiatives; Assistant to the President for National Security Affairs; Assistant to the President for Homeland Security and Counterterrorism; Administrator of the U.S. Digital Service; Administrator of the Office of Electronic Government ("Federal Chief Information Officer"); Commissioner of the Technology Transformation Service; and Director of the American Technology Council ("Director"). *See id.* at §§ 3, 6.

130. *See About CIA*, CENT. INTEL. AGENCY, https://www.cia.gov/about-cia [https://perma.cc/4K6G-9F63] (last visited July 20, 2019).

131. This is in addition to the Armed Forces of the United States in time of war declared by Congress or during any period covered by a report from the President to the Congress under the War Powers Resolution. *See* COMM. ON OFFENSIVE, *supra* note 92, at 291. However, the President could determine that another agency is more likely to achieve the particular objective. *See id.*

132. *Id.* "*Special activities* means activities conducted in support of national foreign policy objectives abroad which are planned and executed so that the role of the United States Government is not apparent or acknowledged publicly, and functions in support of such activities, but which are not intended to influence United States political processes, public opinion, policies, or media and do not include diplomatic activities or the collection and production of intelligence or related support functions." Exec. Order No. 12333, 40 Fed. Reg. 235, § 3.4(h) (December 4, 1981) (emphasis original).

133. *See Our Mission*, U.S. ARMY CYBER COMMAND, https://www.arcyber.army.mil (last visited July 20, 2019). More closely, ARCYBER, the Army headquarters beneath U.S. Cyber Command, "conducts global operations 24/7 with approximately 16,500 Soldiers, civilian employees and contractors" spread across four states. *About Us*, U.S. ARMY CYBER

and Security Command also partakes in cyber intelligence, which includes potential surveillance.[134] Nevertheless, the military, under the President, and the CIA may generate self-regulation to the extent that they establish internal rules regarding the use of their cyber warfare powers.[135] The CIA or the military could also generate indirect regulation, to the extent that they use contracts with third parties who provide it with services to implement regulatory norms.

Expanding the focus beyond the plurality within the federal government reveals the complexity of the U.S. system on two other dimensions: (1) the federal-state axis (states retain regulatory powers relevant to the cyber domain) and (2) the legislative-executive axis (the legislature, whether federal or state, may address cyber risks by legislating norms of behavior that pertain to those engaging in cyber activities). Alternatively, legislatures may shape executive responsibilities and lines of authority. Thus, Congress may decide which agency will be in charge of regulating which cyber activity and to what extent (including which enforcement powers such an agency may have). State legislators are equally important, as criminal and civil liability are often dispensed at the state level, similarly to duties to disclose information. Take for example security breach laws, which exemplify a form of regulation through information. In the United States, "[a]ll 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted [security breach laws] requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information."[136]

COMMAND, https://www.arcyber.army.mil/Organization/About-Army-Cyber [https://perma.cc/78K2-GXE7] (last visited July 20, 2019). It is composed of several units, e.g., U.S. Army Network Enterprise Technology Command, 1st Information Operations Command, 780th Military Intelligence Brigade, Naval Network Warfare Command, Navy Cyber Defense Operations Command, 624th Operations Center (Airforce); and Marine Corps Cyberspace Command. Its main priorities are to: "[(1)] Operate and aggressively defend the Department of Defense Information Network . . . [(2)] Deliver cyberspace effects – both defensive and offensive – against global adversaries . . . [and (3)] Rapidly develop and deploy of cyberspace capabilities to equip [its] force for the future fight against a resilient, adaptive adversary." *Id.*

134. *See Mission*, U.S. ARMY INTEL. & SECURITY COMMAND, https://www.army.mil/inscom#org-about (last visited July 20, 2019). For more on the military in the cyber-context, see Jeffrey L. Caton, *Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications* (Jan. 2015), https://publications.armywarcollege.edu/pubs/2317.pdf.

135. For a differentiation between cyberwarfare, cyberattack, and cybercrime, see Hathaway et al., *supra* note 27, at 833.

136. *State Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES, http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx (last updated July 17, 2020) (full list of states and respective legislation citations available on website). For more on data security breaches, see generally Paul M. Schwartz & Edward J. Janger, *Notification*

Notably, the United States acknowledged that the cyber domain requires developing a strategy on a national level. Under the *National Cyber Strategy*, the United States took action to address cyber threats by "strengthening America's cybersecurity capabilities . . . ."[137] Among other things, this strategy encompasses an administrative understanding of the plurality of regulators, at least to some extent. For instance, to properly secure federal networks and information, it advocates for a plan to "centralize some authorities within the Federal Government, enable greater cross-agency visibility, improve management of our Federal supply chain, and strengthen the security of United States Government contractor systems."[138] It calls for, *inter alia*, "further centraliz[ing] management and oversight of federal civilian cybersecurity"; "ensuring better information sharing among departments and agencies to improve awareness of supply chain threats and reduce duplicative supply chain activities within the United States Government"; "reviewing contractor risk management practices and adequately testing, hunting, sensoring, and responding to incidents on contractor systems"; and ensuring that the "systems [the Federal Government] owns and operates [will] meet the standards and cybersecurity best practices it recommends to industry."[139] Yet the challenges to manage the supply chain are not easy to meet, precisely because each entity has some discretion regarding the technology it uses. Moreover, the federal agencies interact technologically with states and municipal bodies, further complicating the picture.

Consequently, in accordance with the requirements set by EO No. 13800, OMB has published a report assessing government cybersecurity risks, identifying actions to improve federal cybersecurity, and acknowledging cooperation between OMB and other agencies on the implementation of the report.[140] This report reflects on, *inter alia*, ineffective allocations of agencies' limited cyber resources, which resulted in seventy-four percent of the examined agencies implementing "cybersecurity programs that are either at

of Data Security Breaches, 105 MICH. L. REV. 913 (2007) (describing current data security statutes and their incomplete focus on reputational sanctions).

137. *See The National Cyber Strategy*, *supra* note 66, at II. This strategy is aimed to provide methods to "(1) defend the homeland by protecting networks, systems, functions, and data; (2) promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation; (3) preserve peace and security by strengthening the United States' ability – in concert with allies and partners – to deter and if necessary punish those who use cyber tools for malicious purposes; and (4) expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet." *See id.* at 3.

138. *See id.* at 6.

139. *Id.* at 6–8.

140. *See Federal Cybersecurity Risk Determination Report and Action Plan*, *supra* note 82.

risk or high risk."[141] To improve cybersecurity, the report identified "four . . . core actions that are necessary to address cybersecurity risks across the Federal enterprise . . . ."[142] Part of the challenge lies in the limited jurisdiction of OMB itself (and the fact that the government does not necessarily want to "solve" this problem by subjecting all agencies to OMB, for separation-of-powers reasons).

Still, as this Article demonstrates, the plurality of regulators (as broadly defined) is extensive and mostly decentralized. Each department is charged with its own (usually, but not exclusively, defensive) mission, but such regulation radiates to cyber-related activities outside of its domain. This compartmental approach allows for greater understanding of the needs of the specific social field and is aligned with the legal structures underlying the separation of powers, although not without costs.

One major concern within this respect is that agencies are often driven by their own interests without necessarily appreciating the bigger picture. This potential failure to see the bigger picture may be attributed to several factors. One such factor is the difficulty to sustain an overall protective shield over the various agencies (when it is enough that one is compromised to allow access to the whole compromised unit). Another factor relates to the different goals and approaches of each agency. For example, the goals of the NSA—an operative agency—are probably different from those of the FCC—a regulatory agency—and their incentives to actively engage in cyber activities are not identical. Yet, since they operate in the same field, the misalignment among their goals could lead to power struggles between agencies to control such cyber activities (offense, defense, or attack), to the extent these agencies have either direct powers to act or regulatory powers to guide and constrain. Finally, their efforts could overlap many times. The plurality of regulators could lead to confusion as to who protects what, resulting in either no cybersecurity or inefficient overlapping cybersecurity efforts.[143]

---

141. *Id.* at 3.

142. *Id.* These actions include: (1) "Increase cybersecurity threat awareness among Federal agencies by implementing the Cyber Threat Framework to prioritize efforts and manage cybersecurity risks"; (2) "Standardize IT and cybersecurity capabilities to control costs and improve asset management"; (3) "Consolidate agency SOCs to improve incident detection and response capabilities"; and (4) "Drive accountability across agencies through improved governance processes, recurring risk assessments, and OMB's engagements with agency leadership." *Id.*

143. Cybersecurity efforts often overlap. Take for example the protection of oil and gas pipelines controlled by SCADA. Both DHS and DOT were directed to implement a cybersecurity plan, but with confusion as to which agency will lead the effort. To overcome overlaps, Congress tasked DHS to jointly work with DOT (through PHMSA) and private

Initiatives like CERT (where information is meant to be shared by the various participants) are partially designed to harmonize agencies' responses based on shared-threat information and analysis. But information sharing is only one aspect of cyberactivity. Moreover, it is unclear whether such information sharing is sufficient should disagreements persist amongst separately acting authorities. While regulatory sandboxes—where each regulator experiments with various approaches—may be effective as an adaptive process to address ever-evolving threats, it could also lead to, *inter alia*, a waste of resources if different regulators work on the same risk simultaneously without necessarily learning from or cooperating with each other.[144]

The plurality of regulators and actors within the executive also creates coordination problems that could undermine cybersecurity. Some consumers have complained that U.S. CERT warnings "generally arrive a day or two after they might have been helpful."[145] Suppose that a cyberattack on a sensitive government network occurred and that a disclosure of this attack by the investigators, e.g., the FBI, could jeopardize an ongoing investigation.[146] In such a case, the FBI might withhold such information from private parties or even other regulators within the executive, even though this information may assist those other entities in protecting themselves against a similar attack. This becomes even more problematic in the critical infrastructure sector, where most of the actors are usually privately owned.[147]

---

entities in applying the required "Pipeline Security and Incident Recovery Protocol Plan." *See generally* TRANSP. SECURITY ADMIN., PIPELINE SECURITY AND INCIDENT RECOVERY PROTOCOL PLAN (Mar. 2010), https://www.hsdl.org/?view&did=13226; *see also* U.S. DEP'T OF TRANSP., AV-2008-053, ACTIONS NEEDED TO ENHANCE PIPELINE SECURITY (2008), https://www.oig.dot.gov/sites/default/files/Pipeline_Security_Report_reissued_AV-2008-53.pdf.

144. *See generally* Robert Kenneth Palmer, *Critical Infrastructure: Legislative Factors for Preventing a "Cyber-Pearl Harbor"*, 18 VA. J.L. & TECH. 289, 329 (2014) ("There are too many government agencies with different cyber-missions working independently, with project duplication to the point that it is not uncommon for several different groups to be working on the same thing, unaware of each other's efforts.").

145. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-588, CYBER ANALYSIS AND WARNING: DHS FACES CHALLENGES IN ESTABLISHING A COMPREHENSIVE NATIONAL CAPABILITY 41 (2008); *see also* Palmer, *supra* note 144, at 326.

146. *See* Palmer, *supra* note 144, at 327.

147. *See* EXEC. BRANCH OF THE U.S. GOV'T, THE NAT'L STRATEGY FOR THE PHYSICAL PROT. OF CRITICAL INFRASTRUCTURE AND KEY ASSETS 8 (2003), https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf ("Private industry owns and operates approximately 85 percent of our critical infrastructures and key assets."); William C. Banks & Elizabeth Rindskopf Parker, *Cybersecurity Symposium: National Leadership, Individual Responsibility*, 4 J. NAT'L SECURITY L. & POL'Y 7, 9 (2010).

Lastly, looking back at the judiciary also reveals the plurality of courts in the United States—state and federal—which also participates in the formation and enforcement of regulation. As this Article previously argued, when judges are asked to decide cyber-related matters, they effectively regulate, either by infusing norms with practical meaning through interpretation, or by ensuring compliance with higher norms and thereby blocking the application of a regulatory norm or laying out a map for permissible regulation. The plurality of courts in the United States at the federal and state levels is likely to generate some inconsistencies, which may result in a laboratory of sorts but may also increase some risks when a unified and coordinated response is more optimal. While legal diversity and pluralism are features of any legal field in the United States and are usually deliberative cornerstones of the system's resilience and adaptability, the ramifications of potentially vast differences among states (alongside the built-in limited role of federal law) could be significant in terms of offense, defense, and, perhaps most importantly, surveillance.

The networked domain challenges traditional conceptions of jurisdiction by deepening the plurality within the United States, as D2D surveillance activities in one state are unlikely to be limited to its territory, given the structure of the networked society. Such plurality is further expanded as a consequence of the presence of courts outside U.S. jurisdictions, since it is not uncommon that components of the surveillance chain are outside the United States; either some parts of the communication are directed to infrastructure outside the United States, with elements of the data stored outside the United States, or the surveillance operation has a foreign component.[148] Such diversity may lead to conflicting approaches regarding which court has jurisdiction with respect to what. In any event, it is likely to increase the differences in interpretations and application. Such pluralism may lead to a suboptimal "fit" between the various clogs in the regulatory matrix, to the extent that the varying approaches generate negative interferences.[149]

III. PLURALITY OF THE STATE: THE USER AND THE SUPERUSER

When the state acts as a regulator, it shapes the rules of behavior at the constitutional, statutory, and sub-statutory levels and controls the enforcement of rules. The plurality of the state in cyber activities runs deeper, as it goes

148. For more on jurisdiction in the digital era, see generally David R. Johnson & David Post, *Law and Borders-The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

149. For more on the concept of negative interference, see generally Eldar Haber & Amnon Reichman, Regulatory Processes, Attitudes and Modalities: The Complexity of Cyber (Date) (unpublished manuscript) (on file with author).

beyond the plurality of regulations. State agencies perform two other distinct roles: those of a user and those of a "superuser."

As a user, the state relies on digital networks, mainly the internet, like any other user or customer. The state operates and maintains government websites and social media identities. It uses the internet to search, tweet, post, email, and do whatever users do online. In that capacity, the state is the consumer of private software services and hardware products and is expected to abide by license agreements governing social platforms or other networked entities.

But the state is also a different kind of user: *a superuser*. By virtue of its size and abilities, the state can single-handedly affect the terms or conditions of services other users face. It may do so either by wearing its contractual and propriety hat or by donning its executive (i.e., operational) uniform. Relying on its market-based strength, the state may harness its power in private law to shape the contracts it signs, to determine how its property may be used, or to shape the behavior of those who wish to interact with it. In its executive-operational capacity, it may rely on its ability to do things, such as build infrastructure or offer services directly, by asserting its control over the public sector. As mentioned before, the CIA, NSA, and military are superusers in the sense that they have significant resources at their disposal, and their sustained activities, especially if coordinated, may affect many others, if not the whole ecosystem itself. This is because these national security agencies have the power to act directly. They also have the market power to induce firms who wish to engage in commercial transactions with national security agencies to comply with the requirements set forth by those agencies.

The notion of the state as a superuser in cyber holds significant ramifications to the market and to individuals operating within the digital sphere. As noted, through their superuser powers, the state and a small, ever-consolidating cadre of other players[150] construct the networked dimension and communications within that domain. Furthermore, via its algorithmic powers and access to data, the state may generate a unique type of social control in the networked dimension and beyond.

150. *See generally* TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES (2010); TIM WU, THE CURSE OF BIGNESS: ANTITRUST IN THE NEW GILDED AGE (2018); Michal S. Gal, *Algorithms as Illegal Agreements*, 34 BERKELEY TECH. L.J. 67 (2019); Esther Gal-Or & Anindya Ghose, *The Economic Consequences of Sharing Security Information*, *in* 12 ADVANCES IN INFORMATION SECURITY, ECONOMICS OF INFORMATION SECURITY 95 (L. Jean Camp & Stephen Lewis eds., 2004); Daniel Rubinfeld & Michal Gal, *Access Barriers to Big Data*, 59 ARIZ. L. REV. 339 (2017). The penetration of algorithms raises further consolidating concerns as data is consolidated by data-giants. *See generally* Niva Elkin-Koren & Michal Gal, *Algorithmic Consumers*, 30 HARV. J.L. & TECH. 309 (2017).

This is, of course, not to say that the role of a superuser is confined to cyber. The state may, if it so chooses, adopt superuser capabilities in most, if not all, environments because it may use its market size and hierarchical structure to influence the manner in which most other players conduct their business. However, as this Article further shows, in light of the manner and path in which the digital networked domains have evolved, the plurality of the state in cyber is more complex given the interplay between the state's regulatory facets and its role as a user and superuser. Understanding this complexity is crucial for gaining a more comprehensive grasp of the regulatory challenges currently facing technologically advanced jurisdictions.

A. USERS

The ubiquitous role of the state in cyber is as an ordinary user. The term "user" captures both those who consume services or buy products, i.e., customers, and the myriad of small companies who provide or sell services and products (software or hardware). In that sense, the various state entities are part of the social landscape that has migrated to the digital domain. State entities operate within the digital environment just like anyone else when performing in their official capacity. Governments, government officials, law enforcers, and legislators are users of varying digital technologies, ranging from networked (or cloud-based) productivity suits from word-processing to social platforms, the internet more generally, and, of course, communication devices such as smartphones.[151] State entities might operate an official website, use institutional email accounts, and even run official social media identities.[152] They would usually use commercial software and hardware to run their information technology.[153]

Similarly, many officials who use instant messaging platforms in their official capacity may use video platforms to edit and share videos and to generally participate in the creation and sharing of information. Many state agencies rely on online commercial platforms or on components of commercially available digital products in supplying services to the public,

151. The list of state users could be much broader, depending on how we define "the state." Naturally, we could include in such list any state-related employee, e.g., librarians, public school faculty, public university staff, etc.

152. For example, as of now, the White House operates a Twitter account (https://twitter.com/whitehouse), a Facebook account; (https://www.facebook.com/WhiteHouse), an Instagram account; (https://instagram.com/whitehouse), a Flickr account; (https://www.flickr.com/photos/whitehouse), and more.

153. Naturally, the state can order and/or produce software and hardware that is designed and tailored for specific uses and users. Even so, they still rely at least partially on commercial software and hardware.

ranging from billing services (for customers of public utilities or those subject to fines or citations) to registry services (for transactions such as real estate or car sales). Under its role as a user, the state is not generally empowered by its status.

Needless to say, some state networks are closed to the public, but unless the network is fully developed and maintained by the state and operated on state infrastructures, the state is not different in essence from any other corporation running a discrete network. More often than not, the network is maintained by some private corporation or, at the very least, uses commercial software and hardware. The state agency under such circumstances is essentially a client of one or more software and hardware companies from which it buys goods and services.

Digital core government services are becoming an integral part of many states.[154] As part of this move toward digitizing government services, the U.S. Digital Service—a technology unit within the EOP—is tasked with delivering "better government services to the American people through technology and design."[155] To do so, it embeds teams within federal agencies and their in-house digital technology divisions.[156] But more specifically, the state will most likely grant more core services via digital means in the near future, thus expanding its reliance on private entities' infrastructures, knowledge, and expertise on how to best protect the said services. Adding to this move are smart city initiatives—urban areas that rely on Internet of Things (IoT) sensors to more efficiently manage services, assets, and resources.[157]

In other words, as digital technology becomes more integral in everyday life, states continuously grow more dependent on its use. Beyond operating social media accounts, official websites, etc., the state cannot conduct business, or even operate, without relying on D2D technology, which are often developed (and maintained) by third parties. State actors must constantly use privately owned networks, productivity suites (such as Microsoft Office Suite), human resources management software, cellular networks, and phones, to name but a few examples. In that sense, any single government user is technically subject to the terms of use or sale as generated and enforced by the

154. *See, e.g.*, Kok Ping Soon, *Building a public service that is digital to the core*, TODAY (Nov. 21, 2018), https://www.todayonline.com/commentary/building-public-service-digital-core.

155. *Our Mission*, *supra* note 79.

156. *Id.*

157. *See* Michael Batty, *Big Data, Smart Cities, and City Planning*, 3 DIALOGUES IN HUM. GEOGRAPHY 274, 277 (2013); Gabriela Viale Pereira, Peter Parycek, Enzo Falco & Reinout Kleinhans, *Smart Governance in the Context of Smart Cities: A Literature Review*, 23 INFO. POLITY 143, 144–45 (2018).

owner of the service or product. Thus, to the extent that the U.S. President uses Twitter, he may be the head of the executive, but is nonetheless a user from Twitter's perspective. His account may be subject to data collection (surveillance) or vulnerable to hacking, just like any other user. Similarly, when an officeholder uses a cellphone, he is subject to the terms and conditions of various applications on that cellphone, and his data (such as his location) may be detected and collected by third parties, just like the metadata of any other user.[158]

As will be noted below, this does not necessarily leave the state defenseless. If it coordinates its actions, and to the extent that some of its components are not merely users but superusers because of their size or capacity, the state may negotiate special terms under which the products are customized for the state and its agents.

However, in many cases, an organ of the state consists of ordinary users or customers of a publicly available product or service and is thus as vulnerable as any other user. If each state entity—each bureau or municipality, each school board, etc.—acts on its own in this respect, they, like any other user (sometimes much like small companies), are at a disadvantage since their ability to guard against unauthorized surveillance and attacks is limited. The information gap favors the industry: most state entities on their own are not necessarily in a position to fully understand the code, evaluate the degree to which it is safe to use, or understand how it can be manipulated. Since the code now penetrates any and all governmental processes, all state entities are vulnerable to data collection by the companies themselves or by third parties, either with permission by the companies or as a result of a hack.

In fact, the state is probably at a greater risk than other users since it may attract a greater attention of attackers whose motivation for attacking may be financial, symbolic, or simply to cause damage by compromising the data or infrastructure. Such attacks may seek to steal information, demand ransom, or corrupt services, data, or both. This is of particular importance because some state agencies—such as local governments—may lack the capacity to defend themselves properly or may otherwise face budgetary constraints to do so, as their funding depends on political processes that may fail to prioritize cyber defense.

158. Consider, for instance, the data collected by fitness trackers when used by military personnel on active service, which gives away the location of secret army bases. *See* Alex Hern, *Fitness tracking app Strava gives away location of secret US army bases*, GUARDIAN (Jan. 28, 2018), https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.

These attacks are not merely theoretical. In recent years, we have come to witness several ransomware attacks against municipalities and even courts.[159] Some declined payment and sought the assistance of the FBI and Secret Service in response to the attack,[160] while others eventually paid the attackers considerable amounts in ransom, in part because such attacks were covered by insurance.[161] Such incidents reveal conflicting approaches among the various state entities—primarily between state superusers (like the FBI) and users (like municipalities)—which could lead to suboptimal outcomes.[162] Whereas, as a general matter, the FBI counsels against such payments in order to not encourage future attacks, ordinary state users must take into account the disruption of services that may follow a protracted stalemate and the overall expense it may cost to rebuild the infrastructure and retrieve the data (if at all possible) should they refuse to pay. These incidents also reveal how vulnerable the state could become as its diverse organs lack the prowess of the FBI, and in fact may fail to implement simple system updates or upgrades because they may lack relevant protocols—or a playbook—for responding to such attacks.[163] The development and implementation of such protocols often requires a collaborative effort, whereby some agencies rely on the capacities and learn from the experiences of other, more advanced agencies.

Such vulnerability is of significance because it may push state entities to insist on higher, certifiable standards of cybersecurity, which may benefit all users. On the other hand, such standards can usually be provided by larger,

159. *See*, *e.g.*, Liz Farmer, *The Baltimore Cyberattack Highlights Hackers' New Tactics*, GOVERNING (May 30, 2019), https://www.governing.com/topics/public-justice-safety/gov-cyber-attack-security-ransomware-baltimore-bitcoin.html; Lily Hay Newman, *Ransomware hits Georgia Courts as Municipal Attacks Spread*, WIRED (Jan. 7, 2019, 7:49 PM), https://www.wired.com/story/ransomware-hits-georgia-courts-municipal-attacks-spread.

160. *See* Jeff Barker, *Maryland's federal lawmakers seek FBI briefing on Baltimore ransomware attack*, BALTIMORE SUN (May 23, 2019), https://www.baltimoresun.com/politics/bs-md-ransomware-fbi-20190522-story.html. Notably, some municipalities signed a resolution not to pay the attackers. *See, e.g.*, Jacob Solis, *As hackers target U.S. cities, Las Vegas signs on to resolution not to pay future ransoms*, NEV. INDEP. (July 9, 2019), https://www.rgj.com/story/news/2019/07/15/lyon-county-school-district-hacked-latest-local-agency-cyber-attack-cyberattack-baltimore-ransomware/1740490001.

161. *See* Stephen L. Carter, *When It's Worth Paying a Hacker's Ransom*, BLOOMBERG (June 6, 2019), https://www.bloomberg.com/opinion/articles/2019-06-06/baltimore-computer-hack-sometimes-cities-have-to-pay-a-ransom; Tomáš Foltýn, *Two US cities opt to pay $1m to ransomware operators*, WELIVESECURITY (June 26, 2019, 11:05 PM), https://www.welivesecurity.com/2019/06/26/cities-pay-ransom-ransomware-operators.

162. *See* Benjamin Freed, *One year after Atlanta's ransomware attack, the city says it's transforming its technology*, STATESCOOP (Mar. 22, 2019), https://statescoop.com/one-year-after-atlantas-ransomware-attack-the-city-says-its-transforming-its-technology/.

163. *See id.*

more established firms, which may push for further consolidation. If state entities migrate to purchasing services from the larger corporations under the assumption that these corporations are able to maintain higher (and more expensive) cybersecurity protocols, not only is a message sent to the rest of the commercial market, but such a move also empowers the larger corporations by providing them with further business (and thus revenue and control of the market).

More importantly, the vulnerability—real or perceived—of the myriad of state agencies may generate pressure on the regulator to issue regulations to protect these entities as users from potential harm-doers. Recall that the dependency of officeholders as users on technology developed by the industry is only one part of this prong. The fear of such dependency becomes greater due to a gravitation towards consolidation of data, whereas state entities face a relatively small number of very big players, namely superusers. This, in turn, raises an interesting regulatory dilemma: To what extent should the state as a user be singled out for protection vis-à-vis other users (customers and small providers alike)? Relying on established consumer protection legislation may help all users, including state users, but may raise practical questions related to recourse for enforcement mechanisms when a state entity approaches the consumer protection agency with a complaint related to itself as a user. To the extent that the consumer protection agency disagrees with the position of the complaining state agency, it is unclear how such disagreement may be resolved. Similarly, to the extent that the state agency is conceived to be a user, it is unclear whether it can initiate class action litigation on behalf of other users. In any event, as a matter of substance, current consumer protection laws may not be sufficient because the supply chains of technology are complex, and thus the consumer-provider distinction may be less relevant in protecting users against cyber offense and surveillance.

Of particular interest is the protection of various state entities from superusers—corporations or states that possess capacities so great that they may affect the playing field itself. The regulatory dilemma here is also apparent: not only is it less clear that that state as a regulator has the capacity to effectively reign in the superusers, but the state itself is also a superuser. Given the intentional separation of powers and functions among state entities, the state entities as users may find themselves looking for protection from the capabilities of other state entities with the wherewithal to interact with the code or hardware undergirding the networks, and collect, store, and analyze vast amounts of data with or without the full awareness and consent of the users. In other words, state agencies as users may find themselves caught up in the cyber activities of other state agencies in their superuser capacity.

Some state agencies may have at their disposal access to experts and the ability to issue guidelines to their employees, or they may have internal capacity to generate advanced preventative measures against hackers or superusers. Such state entities are at an advantage. On the whole, the bureaucratic structure within which state agencies operate may offer some hope because it allows for instituting systemwide measures. However, the very same structure is usually not known for agility, which in turn may present a challenge. Turning this challenge into an asset requires the state to implement a clear structure of information sharing among various state entities on multiple levels of the government, as well as within the industry, and to harness its more formal lines of communication to implement dynamic prevention, response, and recovery protocols. It still does not protect a state entity as a user from being caught up in the cyberactivity of another state agency with superuser capabilities.

In terms of executing surveillance operations, under its role as a user, the state is rather limited. Admittedly, state officials can use publicly available data or privately shared data (as recipient of such data) like any other user can. But it is only once the state develops superuser capacities, as further discussed below, that the state turns into a full-fledged data-collecting, mining, and analyzing creature.

B. SUPERUSERS

1. Defining a Superuser

A superuser differs from a regular user (consumer or seller) on account of the greater capacities the superuser has. It is therefore a relative term. If all users possess a similar ability, then they are not superusers, but simply users. In this case, more knowledgeable users (who are not quite superusers) might be termed "powerusers."[164] Therefore, the definition of a superuser requires not only power (or even greater power than the ordinary user).[165] Rather, it requires the ability to control and manipulate the options available to a considerable number of inhabitants of the digital dimension, or to otherwise shape the dimension itself by affecting the network, i.e., the digital equipment relevant for cyber activities.[166] Put differently, superusers possess the ability to construct and make changes to segments of the structural design of the digital

164. The terminology of "superuser" was suggested before in academic literature, but it was used to refer mostly to what we call "powerusers." *See* Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. 1327, 1333–34 (2008) (defining "superusers" as powerusers).

165. *See id.* at 1334 ("A person with power X is a Superuser only as long as the percentage of people with X is small."). Such statement is true for both powerusers and superusers under our definitions.

166. *See id.* at 1333 (defining "superusers").

world, or to change the economic and cultural ecosystem within which digital transactions and interactions take place.[167]

Any field of social and economic activity may generate a small cadre of superplayers, depending either on their ability to consolidate power via mergers, acquisitions, and self-development (thereby achieving market dominance) or on their ability to control certain junctures in the ecosystem in a manner that channels activities through their conduits. A unique knowhow, ownership of crucial assets, or preferential treatment by others may play a part in the emergence of a superplayer. Other structural elements, such as high entrance barriers and presence in multiple synergetic markets, may play a role as well. Large-scale availability of human and capital resources—and the ability to harness these resources to achieve focused goals—is usually an ingredient in the making of a superplayer as well. In the cybernetic domain, we refer to such superplayers as superusers, to distinguish them from ordinary users and regulators; however, it is clear that they do not merely *use* preexisting software or hardware, nor are they mere developers. Rather, superusers control significant (namely large and advanced) segments of the development, production, and provision of networked products and services ordinary users rely upon.

One way to situate a superuser is through the paradigm offered by Lawrence Lessig, according to which behavior is regulated via four modalities: legal norms (and practices), social norms, the market, and code (or architecture).[168] A superuser is an entity that has control over at least one such modality to the extent that implementing its policies in that modality affects the behavior of many (if not all) others.

The first modality—regulation through law—is usually performed by the state, typically not as a superuser, but as a law maker, relying on its power to enact primary laws or secondary regulations as norms that apply to all. A closer examination reveals that some entities harness legal arrangements that are not promulgated as norms with general application, but rather norms designed to apply only to specific parties. However, their use may indirectly amount to regulating the many rather than merely the few that are technically bound by such norms. Contracts, including end-user license agreements and terms of use or service, are technically "bilateral" in the sense that they dictate the

167. *See* Robert Bartlett, *Developments in the Law: The Law of Cyberspace*, 112 HARV. L. REV. 1574, 1635 (1999) (arguing that the fundamental difference between real space and cyberspace "is that the architecture of cyberspace is open and malleable. Anyone who understands how to read and write code is capable of rewriting the instructions that define the possible").

168. *See* LAWRENCE LESSIG, CODE: VERSION 2.0 120–37 (2006); LAWRENCE LESSIG, FREE CULTURE 116–73 (2004).

relationship only between the two parties to the agreement. However, mass application of these legal tools amounts to regulating the behavior of all those interacting with these entities. To the extent that an entity has the power to use such contracts and permissions (or similar legal norms) to affect the options, courses of action (and interactions), and horizons (i.e., the perception of what is acceptable or feasible) of many users, such an entity occupies the role of a superuser. Similarly, to the extent that an entity, alone or together with a small group of other entities, may have a significant impact on the creation of domestic or international official (formal) law, the entity may be classified as a superuser.[169]

Superusers can also shape the digital sphere through the second modality, social norms. Given their market share or control of communication nodes, they can reach large audiences and explicitly or implicitly influence opinions and perceptions as well as outlooks, consequently shaping behavior. More specifically, superusers can harness their capacities and effectively convey to users their notion of what should be considered an appropriate, preferable, or, at the very least, acceptable practice (or value or world view). Entities may also resort to less direct ways of communication, including the use of certain graphic designs, music, or video effects; certain sequences of messages; or order in which information is conveyed. To the extent that such entities enjoy hegemony, these less explicit measures may also generate effective social norms.

The third modality is the market. Due to its capacity, the superuser can alter the economic environment and structure of incentives by using forces of supply and demand. Superusers enjoy market domination, which translates to the volume of transactions with multiple players. They can thus set the terms of these transactions. Note that these transactions may be in the line of business of a superuser directly (e.g., transactions between sellers and Amazon) or indirectly (e.g., transactions between those who may supply Amazon with some commodities for its employees).

The same, of course, applies also to the state. Gaining access to the state's supply chains—and thus access to the multiple state agencies and layers of government—could be financially meaningful, whether the supplier is selling beverages, financial services, communication services, technological services, uniforms, or any other item of mass production. In the cyber context, to the

169. Under public choice theory, organized groups with shared interests and defined goals tend to influence legislation more than the public. *See generally* JAMES M. BUCHANAN & GORDON TULLOCK, THE CALCULUS OF CONSENT (1965) (discussing the principles of public choice theory); *see also* DENNIS C. MUELLER, PUBLIC CHOICE II: A REVISED EDITION OF PUBLIC CHOICE 1 (1989) (reviewing public choice theory in literature).

extent that a player controls much of the cybersecurity market as a key buyer of software and computing services (like the state),[170] it obtains the status of a superuser. Beyond the power of deciding which companies will enjoy high revenues from its own purchasing power, the superuser can signal to the market which companies are considered "safe" and trustworthy, but it may also issue warnings against using other companies' services, influencing the behavior and attitudes of many users.[171]

The fourth modality is architecture, or the very code[172] or technical construction of a given social domain. Some entities have the capacity to design the operations of networks, software, and hardware in a manner that impacts the very structure of the environment. They control the way society uses and accesses information, and therefore could use the technical design, interface, and interoperability to implement their policies in pursuit of their goals, even if these policies and goals are not necessarily shared by others. Such capacity is a facet of the superuser status. In the cyber context, superusers may apply their technical capacities for offense, defense, or surveillance. More specifically, superusers can establish technological arms that are dedicated to offense, defense, or modes of surveillance, and then deploy them to such an extent that the operation within the dimension by all, or at least by many, is altered. Alternatively, they may use their power to influence technological companies to use code in a certain manner. Such companies—users or superusers—may be asked, pressured, or required by other superusers (primarily the state) to place backdoors on their devices or networks for use by government officials. The ability to pressure or entice such modes of collaborations is another indication of *de facto* control over the architecture.

2. The State as a Cyber Superuser

The state has the potential to assume the role of a superuser (or superplayer or superactor) in many fields. By definition, when the state acts in its purely

170. In 2004, the U.S. government was estimated to be a consumer of approximately forty-two percent of all software and computing services. The data regarding the percentage of control over the cybersecurity software market might be considered obsolete, but still represents how the state could become a major player as a superuser due to its capacity and purchasing power. *See* BRIAN E. BURKE ET AL., IDC, WORLDWIDE IT SECURITY SOFTWARE, HARDWARE, AND SERVICES 2005–2009 FORECAST: THE BIG PICTURE 1 (2005); Robert W. Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J.L. & PUB. POL'Y 283, 346 (2006).

171. *See, e.g.*, Jordan Crook, *Google Warns Thousands of Users about Potential State-Sponsored Cyber Attacks*, TECHCRUNCH (Oct. 5, 2012), http://techcrunch.com/2012/10/05/google-warns-thousands-of-users-about-potential-state-sponsored-cyber-attacks.

172. *See, e.g.*, Lessig, *The Law of the Horse*, *supra* note 60, at 505–06 (arguing cyberspaces' "architecture is a function of its design.").

executive capacity—building roads, building nuclear bombs, or directly providing a service—it could be seen as a superuser. In its capacity as a regulator, the state can also ensure its monopoly as a superuser (or as a primary superuser in the case of multiple superusers), but it may also decide (or be nudged to decide by political, economic, or technological realities) to allow others to belong to the same club.[173] In cyber, the way this Article has defined it, this potential is salient, and so are the opportunities (and risks) for its use (or misuse).

In fact, the state is probably the ultimate superuser in terms of cybernetic abilities. In offense, there is an indication that states develop the ability to attack multiple destinations, including other states (e.g., infrastructures, governmental platforms, and state-run commercial services), corporations, or "simple" users (i.e., generic users). The state has the capability, either by initiating an attack or by reacting to an attack by others,[174] to disrupt significant portions of networked activities and thus inflict considerable damage.[175]

In terms of defense, it appears that states are developing capabilities to defend critical components, such as military installations, by deploying sophisticated measures that are not necessarily available in the free market. The state also has the capacity to invest in defending other, less critical assets, in a way that need not fall below the standard of other superusers. Finally, as is apparent from various revelations, the state can engage in large-scale or pin-pointed surveillance and espionage operations. It may in fact establish structures that consistently monitor massive amounts of communication

173. A famous example is the production of dynamite, invented by Alfred Nobel, produced by Dynamit Nobel AG, founded in 1865 in Germany, and still producing explosives. *See, e.g.*, Josefin Sabo & Lena Andersson-Skog, *Dynamite Regulations: The Explosives Industry, Regulatory Capture and the Swedish Government 1858–1948*, 23 INT'L ADVANCES IN ECON. RSCH. 191, 194 (2017) (arguing that the Nobel Dynamite Company was able to effectively capture the regulator in part because "[w]ith the new explosives, nitroglycerin and dynamite, the government became dependent on the Nobel company to provide technical, practical and managerial expertise in building a new regulatory framework needed for the growing industry"). On the transnational scene, Nobel Dynamite signed contracts with Du Pont, thereby creating a powerful cartel. *See* GEORGE STOCKING & MYRON WATKINS, CARTELS IN ACTION: CASE STUDIES IN INTERNATIONAL BUSINESS DIPLOMACY 440 (1946).

174. If the state considers cyber attack as a *casus belli* just as any act of war, then retaliation by cyber-means are plausible. *See* David E. Sanger & Elisabeth Bumiller, *Pentagon to Consider Cyberattacks Acts of War*, N.Y. TIMES (May 31, 2011), http://www.nytimes.com/2011/06/01/us/politics/01cyber.html?_r=0.

175. Consider the NotPetya cyberattack, which some attributed to Russia, acting against, *inter alia*, Ukraine. This attack allegedly resulted in more than ten billion dollars in total damages. *See* Mike Mcquade, *The Untold Story of NotPetya, The Most Devastating Cyberattack in History*, WIRED (Sept. 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

across different platforms (and in networks owned by private entities), analyze the data, and generate assessments of its meaning (including probabilistic analysis or profiles of individuals). Since data is data and the power of analytics comes in part from cross-referencing data, the logic of the cybernetic surveillance apparatus is premised on covering more, and preferably all, data points, regardless of originating jurisdiction or whether private or commercial.

The state is a superuser on account of several factors corresponding with Lessig's modalities outlined earlier. The first factor relates to the state's capacities as an actor, which affect the market and the architecture. The state has at its disposal the potential to access considerable budgets and human resources. These can be harnessed to achieve desired goals if the state aligns its bureaucratic structures accordingly. It may thus allocate substantial sums for cyber purposes; invest in cyber research; hire specialists; acquire expensive defense, offense, and surveillance software, hardware, and knowhow (practices and protocols); and build its human capital. This muscle may then be deployed at will. In that context, it should be recalled that governments could also partly or fully own corporations with cyber presence, whether for offensive or defensive technologies and networks, or operators of critical infrastructure.[176]

Put differently, the state can emerge as a powerful—if not the most powerful—player simply because of its size (and hierarchical structures). This power can then be put to design and implement certain architectures. The state may decide to harness its capabilities to construct critical infrastructure or otherwise provide direct services, which may be offered to others (primarily in the defensive theater). It may build such architecture to address its own needs by channeling all internal modes of interaction via certain software or hardware platforms. But given its size and reach, these platforms may affect others to the extent that all interactions with the state are similarly regulated through state-controlled architecture. Needless to say, the state may also decide to buy such architecture or components from others; given its size, such purchases may influence the market (and the architecture therein), as they may affect prices for other users (to the extent that research and development and some

176. Some cities, for instance, are in control of internet infrastructures (i.e., municipal broadband), meaning that these networks are state-operated and owned. *See* Tom Reynolds, *The Failures of Government-Owned Internet*, FORBES (Apr. 26, 2016), https://www.forbes.com/sites/realspin/2016/04/26/government-owned-internet-failure/#5b2a56fa55e2. An example in the context of critical infrastructure is Amtrak, a for-profit corporation and American passenger railroad service that is partially government-funded and founded by the Rail Passenger Service Act (RPSA), Pub. L. No. 91–518, 84 Stat. 1327 (1970). *Amtrak Facts*, AMTRAK, https://www.amtrak.com/about-amtrak/amtrak-facts.html (last visited July 20, 2019).

initial production prices were absorbed by the state). It may also signal to the market regarding appropriate standards, thus saving users information costs.

The size (and organization) also matters when the state interacts directly with others. The state buys (and sells) large amounts of goods and services and may own a considerable amount of property (real or otherwise). As such, it has the ability (if it is able to coordinate its actions) to influence other entities to work with it under its own terms by virtue of its market share. In so doing, it may also harness the legal modality, but as a superuser (as distinct from a regulator). Rather than legislate, it can rely on private law tools. Governmental contracts are a good example. In collaborating with private enterprises (or enterprises owned, fully or partially, by other states), the state can require companies to hand over information in exchange for government contracts.[177] The example of Qwest, a major telecommunications company, is pertinent. When it refused to hand customers' information to the NSA without a warrant, the government warned Qwest that such refusal could negatively impact Qwest's chances to get future classified work with the government.[178] Similarly, the state may require any contractor who wishes to do business with it to comply with certain cybersecurity standards,[179] thereby affecting the market. Contractors are not obliged to work with the state, but the economic incentive might be strong enough for them to align with the protocols set out in state contracts.

Beyond harnessing market forces via contracts, the state can incentivize market players by granting access to state resources (i.e., property). The state, for example, can hand out various digital means at no charge, all without strings attached. Such digital means could include free software, e.g., antivirus software, computer hardware, and even free subscriptions to networks. Such action by the state impacts the ecosystem within which other entities operate,

177. *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1095–96 (2002) (giving ChoicePoint as an example of a private sector company that has contracts with federal agencies).

178. *See* Leslie Cauley, *NSA has Massive Database of Americans' Phone Calls*, USA TODAY (Nov. 5, 2006, 10:38 AM), http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm. A former Qwest executive later alleged that the government withdrew opportunities for contracts worth hundreds of millions of dollars due to Qwest's refusal to participate in such partnership with the NSA. *See* Ellen Nakashima & Dan Eggen, *Former CEO Says U.S. Punished Phone Firm*, WASH. POST (Oct. 13, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202485.html.

179. *See, e.g.*, *The National Cyber Strategy*, *supra* note 66, at 8 ("The Federal Government will ensure the systems it owns and operates meet the standards and cybersecurity best practices it recommends to industry. Projects that receive Federal funding must meet these standards as well. The Federal Government will use its purchasing power to drive sector-wide improvement in products and services.").

as these incentives could enhance the state's ability to control what individuals use and their level of cybersecurity. Perhaps most importantly, it could grant state surveillance capabilities.

Finally, the state is a superuser not only because it has executive prowess—or the ability to act in cyber directly—or economic clout, which affect the architecture and the market (sometimes via legal tools, such as contracts and property). It also has access to symbolic resources, which harness and shape social norms. Bluntly put, the state can resort to the patriotic sentiment (or commitment) to achieve some of its goals or otherwise use its educational capacities as a generator of collective narratives. To the extent that a certain issue is framed as a matter of national security, state organs may rely on their mandate (and framework narrative supporting this mandate) to protect the state's citizens. As gatekeepers whose role is to ensure that "We the People"[180] are safe, they may appeal to others, users and superusers alike, for aid in achieving this collective goal. In the United States, this occurred in the aftermath of the September 11 attacks when companies, which had prior to the attacks refused to hand information to the government, changed their attitudes.[181] More generally, the cybersecurity industry often shares the attitude of state organs regarding the importance of maintaining national security (and to that end, maintaining the necessary technological edge via research and development, offensive cyber espionage, and cyber defense). Sharing the social norms is also reflected in the market. It is not unusual for personnel to migrate from the industry to the state and back, as part of a sub-ecosystem working in offense, defense, or surveillance.

As the previous paragraphs reveal, the state is in a unique position in part because it can leverage one modality with the others—the law (private law, but also public law, as will be discuss below) with market share, with social norms, and with direct (executive) influence over the architecture (code). This convergence is relevant to cyber. Through this convergence of modalities, the state seeks control of the key component of cyber: data. Offense, defense, and surveillance are all about data—disabling it (or disabling hardware through it), protecting it, or learning about it. The state is therefore a unique superuser in so far as it is able to access data with respect to other players (individuals, firms, non-governmental organizations, or agencies of other states), which the state can obtain when such users use its numerous platforms or receive or get such data from other users or superusers (voluntarily or less so). The state is also unique in its ability to obtain data about the architecture and code itself (from various sources). The ongoing automatic (machine-based) access to vast

180. U.S. CONST. pmbl.

181. *See* Solove, *supra* note 177, at 1097.

amounts of data, the ability to continuously analyze the data, and the ability to track changes to the infrastructure itself all place the state in a unique position.

Naturally, the state is not the sole superuser. Depending on various factors, as further suggested, other players could (and have) become superusers much like the state, perhaps with even greater powers than the state under some circumstances. First, other states could be superusers as well. Notably, not every state automatically becomes a superuser simply by virtue of being a state. Some states are powerusers or simple users, as they lack the relevant resources and expertise. Nevertheless, superuser states do exist, and such states could use their power to either collaborate with or fight against other superusers. Second, companies could be superusers as well. As noted above, and given the hyper-consolidation of mass players,[182] Google, Microsoft, Facebook, Apple, Amazon, Intel, and other major technology conglomerates like Cisco are not ordinary players (or simple users). They play a significant role in constructing the ecosystem itself. Communication companies could also become superusers to the extent that they dominate a segment of the networked dimension, so that their conduct and policy require others to align accordingly or suffer the consequences.[183] Finally, while probably rare, coalitions of individuals could also become superusers. Here, we do not refer to the sole hacker, even if he can hack into highly secured systems. It requires more than that. But, a large operation of skilled individuals—hacking collectives—that can manipulate data and networks could constitute a superuser (to the extent that this association can join forces and act in a coordinated manner in a given incident).

To be sure, the discussion about the state as a superuser does not assume that all entities of the state achieve superuser status. In fact, the analysis is sensitive to the multiplicity of the state, whereby segments of the state can enjoy superuser status, while other segments of the state remain mere users. It is this potential tension within the state and among state agencies that may generate opposing pulls between the state as a superuser and the state as a user, thereby posing a regulatory dilemma to yet other segments of the state, namely those performing a regulatory role. However, at some level, the superusers and the regulators are also users to the extent they rely on unmodified commercially available networked services and products, as they often do. So

182. *See* WU, THE MASTER SWITCH, *supra* note 150, at 269–300 (describing the ascendance of the Apple into market dominance by aligning itself with AT&T); Gal & Rubinfeld, *supra* note 150, at 369–70 (addressing the entry barriers in big data markets and the advantages these may generate to big data players).

183. *See, e.g.*, Josh Dzieza, *Prime and Punishment*, THE VERGE (Dec. 19, 2018), https://www.theverge.com/2018/12/19/18140799/amazon-marketplace-scams-seller-court-appeal-reinstatement (demonstrating Amazon's powers).

the distinction may not always be clear cut. Moreover, in regulating superusers, the regulatory segments of the state realize that they may capture the superuser segments of the state as well as market-based corporations. This raises the question of whether, or to what extent, the state should be exempt from superuser regulation, and, if so, what alternative checks should be placed on the superuser capabilities of some state agencies, as long as checks and balances matter.

3. The State as a Superuser in Cyber: Maintaining the Status

There is a strong reason to believe that the state wishes to maintain its status as a superuser, given the power it entails to pursue policies. With respect to some offensive, defensive, or surveillance derivatives, it may also wish to be the *sole* superuser to the extent that it deems it necessary. As hinted, the state may use its regulatory powers or its economic capacities to achieve such exclusivity. On the other hand, the state does not necessarily wish to remain the sole superuser in all dimensions of the cyber market. As detailed below, the presence of other superusers can be beneficial for the state in its capacity as a superuser. The state's goal to maintain its status requires, therefore, a strategy played in three planes: vis-à-vis users, non-state superusers, and other state superusers.

Users do not pose a great threat to the superuser (save for the threat to its economic model, including its reputation). As noted, the reverse is not true, which may raise calls for exercising regulatory control over the superusers. At the same time, users may become powerusers, thereby exercising a checking function on the activities of others in cyber, or even, in rare cases, a potential superuser. Therefore, the state has an incentive to monitor the identity, or at the very least the quantity, of superusers (or those with the potential of becoming a superuser) in order to maintain its relative status. The obvious way to accomplish this is by using its role as a regulator. But as a superuser, it could also try to make sure that other users, mainly powerusers, do not accumulate enough power to become superusers in a manner unsupervised by the state. It could, for instance, use its market powers to signal to powerusers what technology they should use if they wish to interact with the government, thus shaping their cyber capabilities.

As for other superusers, the analysis is more complex. After all, the migration of commercial, social, and cultural activities to the virtual domain—which opened up the opportunity for the state to be a superuser in that domain (and which advances economic growth and, ostensibly, general welfare)—relies on there being a vibrant environment that provides added values to users. This construction of, migration to, and rapid evolution of digital goods and services relies in no small part on market-driven innovation. Had the state kept

the digital networks as part of the public sector, it is less likely that the internet as we now know it would have emerged. Since it appears that there are advantages to size in data analytics, a key feature in the digital economy, it is not surprising that consolidation emerged and superusers were formed.[184] We do not suggest that the emergence of superusers was or is necessarily inevitable, and we cannot imagine a vibrant, robust virtual dimension without the consolidation currently witnessed. But to the extent that consolidation emerges and such consolidation does provide some benefits, the state has an interest in ensuring that the ecosystem is maintained and, more importantly, that the state may enjoy a degree of cooperation with other superusers.

At the very least, the state has an interest in maintaining the ability to access the data of the other superusers—if such a cooperation is not forthcoming—via maintaining the state's technological superiority, or by taking advantage of the presence of national security machinery, which it executes under a different regulatory regime. Companies like Google and Facebook (i.e., other superusers) hold vast amounts of information and thus present a site for datamining from the perspective of the state—an opportunity that was perhaps more difficult to realize when such companies lacked their status as superusers.

Put differently, the presence of other superusers could lead the state to act against them (as the other superusers may target the state as a superuser), but not necessarily. Acting as the sole superuser in cyber could be less optimal for the state because cooperation may be preferable, provided the state has at its disposal mechanisms to preserve its relative advantage. The authors term this balance of power as premised on the concept of "zone of tolerance"[185]—

184. *See generally* WU, THE MASTER SWITCH, *supra* note 150 (describing the cyclical dynamics of the communication sector, where technologies and players emerge as a promise for diversity and freedom, then go through processes of consolidation, in part in an effort of tycoons to achieve control and in part as the economic incentives push for concentration, until a new technological revolution reshuffles the deck); John M. Newman, *Antitrust in Digital Markets*, 72 VAND. L. REV. 1497, 1548 (2019) ("Some argue that digital markets offer unique procompetitive benefits, but a closer look demonstrates that these purported efficiencies tend to be illusory . . . or rife with anticompetitive potential."); Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON L. REV. 1009, 1024 (2013) ("But behind the surface diversity there is ever more concentration of activity in a small group of platforms that know ever more about their users."); Randall C. Picker, *Competition and Privacy in Web 2.0 and the Cloud*, 103 NW. U. L. Rev. COLLOQUY 1 (2008) (arguing that privacy laws restricting the sharing of information across firms but not within segments of the same firm may undermine competition by incentivizing consolidation); Lina M. Kahn, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710 (2016) (arguing that antitrust laws in their current format are ill-equipped to address multi-dimensional online corporations which enjoy a big-data advantages).

185. This term was based on the work of Walton Hamilton. *See* Walton Hamilton, *Institution*, ENCYCLOPAEDIA OF THE SOCIAL SCIENCES VOL. VIII, 84, 236 (Edwin R. A.

according to which the state can tolerate the existence of other superusers, but only so long as these superusers are not more powerful than the state. Similarly, to the extent that the other superusers may coalesce (or if one such superusers becomes strong enough on its own), the superusers may seek to inhibit the powers of the state as a superuser (or as a regulator).

The state resorts to several tactics in order to maintain such a zone of tolerance. Aforementioned is the use of contracts, which is one way to reduce competitors or economically strengthen a player with potential to become a superuser. For instance, if the state grants its citizens free telecommunication services, it will likely greatly affect the feasibility of any provider in that market to compete. Less dramatically, the state may cultivate supported industries of private companies that assist the state in maintaining its technological capacities. The state may flex its human resources muscles by developing offensive, defensive, or surveillance capacities on its own to safeguard its assets and obtain assets of others. To the extent that the state augments its capacities, it affects the state's potential for action against other superusers. Alternatively, it may actually exercise such a potential against hackers—superusers or powerusers—thereby signaling its presence in the ecosystem. More specifically, the state could act aggressively against hackers by cyberattacking them or retaliating when attacked. It could also resort to its enforcement capacities and either indict the hackers or inflict economic or travel sanctions to the extent that the identity of the hackers is revealed.

Finally, the state must confront other states (in their capacities as superusers). The virtual dimension (which includes the networked economy, social platforms, and physical infrastructure) is transnational (or global), and therefore the existence of other state superusers is a given feature of the system. Like in the case of non-state superusers, it is not clear that any single state would pursue a strategy of seeking worldwide exclusivity, as this strategy may either be unrealistic or unproductive (or both). Intelligence, for example, could work better when foreign agencies collaborate.[186] Nevertheless, it is

Seligman & Alvin Johnson eds., 1932); s*ee also* Walton H. Hamilton & George D. Braden, *The Special Competence of the Supreme Court*, 50 YALE L.J. 1319, 1343 (1941).

186. One example of such collaboration was a program named "MUSCULAR"—a surveillance project operated by the NSA and the British Government Communications Headquarters (GCHQ). This project operated overseas in Britain and exploited data gathered from links between Yahoo! and Google's data centers, including both metadata and content like audio, video, and text. *See* Mark Jaycox, *Three Leaks, Three Weeks, and What We've Learned About the US Government's Other Spying Authority: Executive Order 12333*, ELEC. FRONTIER FOUND. (Nov. 5, 2013), https://www.eff.org/deeplinks/2013/10/three-leaks-three-weeks-and-what-weve-learned-about-governments-other-spying; Barton Gellman & Ashkan Soltani, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, WASH. POST (Oct. 30, 2013), http://www.washingtonpost.com/world/national-security/nsa

reasonable to expect that each state would seek to maintain a relative advantage and thus to establish for itself a zone of tolerance with respect to capacities or the actual exercise of cyber powers by other states. The state can use its political or economic strength to coerce some countries to either act in a certain manner or sign a cyber agreement and/or treaty,[187] or the state may even resort to direct action.[188]

All in all, the functions the state plays in the cyber domain are more complex than one might suspect. Beyond acting as a regulator, the state performs two other distinct roles: user and superuser. Offering a taxonomy of the plurality of roles the state plays in cyber is crucial for revisiting one's understanding of cyber regulation. Due to the complexity of such relationships, we now turn to offer several components that should be evaluated in cyber regulation.

IV. REGULATING CYBER-PLURALITY

This Article has established that the state is plural in at least two dimensions: it is both an actor and a regulator. As an actor, it is both an ordinary user and a superuser (with market, technological, and executive powers). As a regulator, it is not one, but many. Consequently, "the state" is subject to potentially conflicting sets of pressures as users and superusers may have different interests. These interests may then be in tension with those represented by the state as a regulator, and, within the regulatory sphere, different regulators may prioritize their varying goals and use different

-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

187. Take the debate on nuclear weapons as an example. The Nuclear Nonproliferation Treaty entered into force in 1970 and rose from an international effort to prevent the spread of nuclear weapons. *See* Treaty on the Non-Proliferation of Nuclear Weapons, *opened for signature* July 1, 1968, 21 U.S.T. 483, 729 U.N.T.S. 161 (entered into force Mar. 5, 1970). While the treaty authorizes five nuclear weapons states (under the pillar of "non-proliferation"), other states are generally restricted to obtain similar capabilities. *Id.* Similar action by the United States (or potentially other states) could arise also in cyber. For more on the Nuclear Nonproliferation Treaty, see generally Orde F. Kittrie, *Averting Catastrophe: Why the Nuclear Nonproliferation Treaty is Losing its Deterrence Capacity and How to Restore it*, 28 MICH. J. INT'L L. 337 (2007).

188. In response to the cyberattack against Sony Pictures in 2014, President Obama publicly blamed and condemned North Korea, and the administration announced new financial sanctions on the North Korean government. *See* Ellen Nakashima, *Why the Sony hack drew an unprecedented U.S. response against North Korea*, WASH. POST (Jan. 15, 2015), https://www.washingtonpost.com/world/national-security/why-the-sony-hack-drew-an-unprecedented-us-response-against-north-korea/2015/01/14/679185d4-9a63-11e4-96cc-e858eba91ced_story.html?utm_term=.05d920a04c2d.

approaches to achieve these goals. Thus, cyber regulation presents a unique test case of how the different functional roles of the state come into play.

Regulating cyber-plurality must therefore first acknowledge this functional separation of powers and the polycentricity that follows, as will be addressed below. Secondly, for cyber regulation to be coherent, regulators (as well as users and superusers) ought to realize that the subject matter expands beyond regulating defense through cybersecurity measures. There have been attempts to regulate cybersecurity at the federal level, mainly through the creation of CISA, but regulators must also be mindful of the fact that such relation should also include the regulation of offense and surveillance. As a matter of technology and the logic of its use, these aspects are interrelated; regulating one aspect without the other would likely yield suboptimal results as technologies migrate and intersect.

What, then, follows from the polycentricity identified in this Article? At a basic level, it seems that there will not be a one-size-fits-all solution to cyber regulation.[189] It is less likely that generating a unitary, comprehensive set of rules, as complex as they may be, will address the concerns of the multiple regulators, the state as a superuser, and the various state entities that use networked products and services and are thus subject to cyber threats. At the same time, this should not be read as a license for a patchwork approach lacking any coordinated structure. If anything, the plurality of the state highlights the need for a collaborative approach between the various agencies at the state and federal levels, one that represents all three functional roles of the state.

Collaboration entails two components: decentralization and coordination. While collaboration is premised on a joint venture framework in which different entities work together on a shared project, nonetheless a degree of decentralization is maintained as collaboration is different from consolidation. The various state entities should not forsake their unique perspectives, not only because it is unrealistic to reconfigure the state into a uniform and fully cohesive body, but because it is a good idea to retain a certain degree of separation of functions and powers. Over-consolidation may negatively impact the manner in which cyber risks are addressed, because such a consolidation may result in conformity and single-mindedness. More specifically, one of the main problems with having one central agency control cyber regulations is the

189. *See, e.g.*, Kenneth A. Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L.J. 377, 387 (2006) ("One-size-fits-all rules cannot easily account for the ways in which risk manifests itself differently across firms.").

lack of diversity in approaches.[190] Heterogeneity could be highly important in forming cyber regulation (cyber action), to the extent that such heterogeneity leads to redundancy, thereby ensuring that if one protective measure fails, others are in place.[191]

Perhaps more importantly, over-centralization may negatively impact the quality of the democratic foundation of the state. Over-consolidation of power in matters of cybernetic defense, offense, and surveillance may be detrimental to the dynamics of accountability, representation, and participation, so central to democratic politics and the liberal, market-based society alike.[192] The concentration of information, knowledge, and decision-making within one entity could thus be proven too risky.[193] Rather, devising structures and processes to allow various perspectives and diverging viewpoints to be represented seems like a more promising avenue, as it could yield informed and considered approaches to cyber threats while maintaining a degree of diversity of opinions and counter-pressures.

Coordination—the second component of the collaborative model—entails an ongoing exchange of ideas and concerns among various agencies and departments in each of the basic stages of the policy formation process. This process comprises of the establishment of factual basis, evaluation of possible regulatory responses, cost-benefit analysis, and devising enforcement/ compliance strategies. With respect to each of these stages, representatives of users, superusers, and regulators should be invited to the table. Practically, therefore, there has to be such a table, namely an institutional platform—perhaps a consortium of various agencies—where such conversations can take place. The various entities do not have to agree, as long as the sources of disagreements are considered.

190. *See* Yochai Benkler, *A Public Accountability Defense for National Security Leakers and Whistleblowers*, 8 HARV. L. & POL'Y REV. 281, 295 (2014); Eldar Haber & Tal Zarsky, *Cybersecurity for Infrastructure: A Critical Analysis*, 43 FL. ST. L. REV. 515, 571 (2017).

191. See, for example, the "WannaCry" virus which spread in more than 150 countries in a matter of hours, encrypting hundreds of thousands of computers (including hospitals), all because of the use (and not patching) of Microsoft Windows. *See* Zak Doffman*, Urgent Cyber Warning for Hospitals Over Threat of 'WannaCry Repeat': Report*, FORBES (July 6, 2019), https://www.forbes.com/sites/zakdoffman/2019/07/06/hospitals-issued-urgent-cyber-warning-over-repeat-wannacry-threat-report/#3724ae026dbf. For a similar argument, see Haber & Zarsky, *supra* note 190, at 572. Notably, centralized cyber regulation could also promote such heterogeneity because an entity with central position "can indeed assure that different cybersecurity measures are applied at different junctures." *Id.*

192. *See supra* all sources in note 20.

193. *See* Haber & Zarsky, *supra* note 190, at 559.

The sharing of knowledge and expertise, which no single entity—let alone the state—could hold on its own, therefore plays a major role.[194] The importance of open and continuous channels of communication, used with the understanding that all participants are working towards better regulation of defense, offense, and surveillance, increases even further if one subscribes to the decentralized and heterogeneous notion described above. Decentralization carries a risk that one segment of the system—one link in the chain—will generate suboptimal regulation (or action). Since all segments of the system are linked, such suboptimal regulation can cause far more extensive damage than failed regulation due to interdependency.[195] Lacking a single authoritative source for cyber regulation could thus result in confusion, inconsistency, gaps, and overlaps.[196] Coordination—understood as a set of processes and institutional culture whereby the various entities carry out their individual duties within a shared framework—stands to mitigate this risk, at least to some extent.

As a matter of jurisdiction, coordination begins at the transnational level, as offense, defense, and surveillance are transnational activities. It is not surprising, then, that the National Cyber Strategy calls for strengthening international cooperation in investigating malicious cyberactivity.[197] But by definition, a National Cyber Strategy is a necessary but insufficient ingredient in establishing a workable transnational structure of coordination. Such a structure, it would seem, would require platforms that ensure ongoing exchanges on devising a transnational strategy (rather than merely a U.S. strategy), as well as expanding its scope beyond investigation and forensics (though this is a good area with which to start). At the national level, the strategy requires cross-agency and cross-industry collaboration with the understanding that while each entity retains its jurisdiction, so to speak, its

194. *See id.* at 560.

195. A good example of interdependency is the U.S. electric grid; a shutdown caused by poor regulation could negatively impact many other services that depend on electricity. *See id.* at 547. A recent example of such interdependency is an attack against "the servers of Dyn, a company that controls much of the internet's domain name system (DNS) infrastructure." Nicky Woolf, *DDoS attack that disrupted internet was largest of its kind in history, experts say*, THE GUARDIAN (Oct. 26, 2016), https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet. This cyber attack, through what was called the "Mirai botnet," brought down many websites including Twitter, the Guardian, Netflix, Reddit, CNN and many others. *Id.*

196. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-10-628, CRITICAL INFRASTRUCTURE PROTECTION: KEY PRIVATE AND PUBLIC CYBER EXPECTATIONS NEED TO BE CONSISTENTLY ADDRESSED 15 (2010), https://www.hsdl.org/?view&did=20017. For more on the problem of centralization, see Haber & Zarsky, *supra* note 190, at 559.

197. *See The National Cyber Strategy*, *supra* note 66, at 11.

concern should be at least recognized by other players. As for cross-agency interface, the National Cyber Strategy has indeed recognized the need for coordination between cyber-related agencies and departments, at least at the federal level.[198] Under this strategy, the NSC is tasked to coordinate with departments, agencies, and OMB on an appropriate resource plan to implement the strategy.[199] The United States has also recognized the need to "identify and bridge existing gaps in responsibilities and coordination among Federal and non-Federal incident response efforts and promote more routine training, exercises, and coordination."[200] The strategy also seeks to provide DHS with "access to agency information systems for cybersecurity purposes and can take and direct action to safeguard systems from the spectrum of risks."[201] This form of collaboration does include a consolidation of some powers, which immediately raises concerns for oversight.

Oversight is the second main regulatory feature that stands out when we recognize the polycentricity of the state. Collaboration, with its two prongs coordination and decentralization, is insufficient if there are no mechanisms of oversight, charged with ensuring that the exchange of information and analysis required for coordination take place, while at the same time ensuring that a certain degree of decentralization is maintained by blunting processes of over-consolidation. Oversight is especially important for detecting capture of the collaborative processes by superusers. The state as a superuser enjoys an advantage because it has direct access to the executive power, and some actions are reserved for the executive alone. To the extent it does not enjoy a technological or market-based superiority, it may seek to harness its executive power to squeeze other superusers out. Such strategy risks downgrading cybersecurity not only because the superusers enjoy a considerable degree of expertise, but because over-consolidation of any technology, including cybersecurity, risks stagnation. The presence of another superuser is thus important because it may contribute to innovation[202] and serve as a check on the power of the state as a superuser.

198. *See id.* at 17.

199. *Id.* at 3. Also, the Federal government is tasked to "the private sector to manage risks to critical infrastructure at the greatest risk," and to work closely with Information and Communications Technology (ICT) providers, to improve ICT security and resilience. *Id.* at 8–9.

200. *Id.* at 8.

201. *Id.* at 6.

202. Government regulation may spur private companies to innovate. *See, e.g.*, Therese Kerfoot, *Cybersecurity: Towards A Strategy for Securing Critical Infrastructure from Cyberattacks* 9–10 (2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2285587. However, the extent

Alternatively, the state (or a segment thereof) as a superuser may seek to collude with other superusers in ways that are detrimental to users (consumers and small producers alike), thereby undermining consumer protection and hindering competition and innovation. Or it may collude in ways that frustrate the goals of regulators, thus evading compliance. More specifically, while collaboration is important, it could also lead to undue influence by the powerful.[203] This could lead to pressures from strong market players (i.e., the superusers) to select certain technologies based on skewed measures, or to hinder the position of their competitors (potentially other superusers) by imposing regulations that burden them (or by otherwise gaining exceptions from burdensome regulations).[204] Substantively, such oversight procedures must only entail the ability to check for conformity with constitutional and statutory normative concerns. Some of the challenges facing any rigorous mechanisms of oversight are obvious: they only add to the institutional complexity, and in cyber regulation dealing with offense, defense, and surveillance, the primary functional logic of oversight—transparency—is not fully available. There is little doubt that at least some level of secrecy will play a part in almost any cyber-related regulation. Some argue that secrecy could promote security,[205] and that public knowledge of the use of certain cyber measures—especially pertaining to operational knowledge regarding attack, defense, or surveillance—could backfire against the state, superusers, and users.[206] Others have questioned the effectiveness of secrecy in promoting security.[207]

Be that as it may and conceding that some secrecy is inherent in matters related to national security and public safety, the dangers of over-shielding cyber regulation from oversight cannot be ignored. The state as a regulator, user, and superuser, directly and indirectly impacts the extent to which fundamental rights, guaranteed by the federal and state constitutions, are meaningfully protected. Moreover, oversight is critical for regulatory impact

---

to which such regulation may indeed do so depends, at least in part, on an ecosystem not fully dominated by a government that controls the development of new technologies as a superuser.

203. *See* Haber & Zarsky, *supra* note 190, at 562.

204. *See id.* at 563 (articulating this concern as "regulatory incitement").

205. *See, e.g.*, Benkler, *supra* note 190, at 294 ("Even if we understand that the national security establishment can make mistakes, there remains the argument that secrecy is vital to security; that the price of transparency is too high.").

206. Some argue that secrecy could be "an essential tool for enhancing security." Peter P. Swire, *A Model for When Disclosure Helps Security: What is Different About Computer and Network Security?*, 3 J. ON TELECOMM. & HIGH TECH. L. 163, 167 (2004).

207. For a discussion on secrecy in the context of cyber regulation, see Haber & Zarsky, *supra* note 190, at 570.

assessment (RIA)[208]—a determination of whether certain regulations indeed achieve their purpose and are cost effective. This is particularly important in a polycentric setting, where the intervention of one agency may overlap with the intervention of another or may depend upon the input of a third. Such oversight is therefore an important quality assurance mechanism.[209]

The practical challenge associated with oversight is devising the proper processes within each agency. Another is proper institution at the inter-agency level. Oversight must have both access to relevant materials and the competence (legal and professional) to audit the collaborative processes appropriately, as well as generate operationalizable advice. Comparative law may yield interesting insights.[210] Courts obviously play an important part, but judicial review, as we know it, was not designed to check offense, defense, and surveillance in cyber. Cyber activities present a challenge: since evidence of such activities is difficult to find, the timeline of activities is such that review may arrive, if at all, a long time after the fact. Additionally, technological expertise of judges is still lacking. Moreover, cyber activities are often accompanied by claims for secrecy, thus prompting the creation of special courts or, at the very least, special procedures.[211] In any event, as oversight mechanisms are developed, it is crucial to ensure oversight of superuser regulation much like of others. This oversight mechanism is important to mitigate unjustified institutional bias on the part of the regulator, which may unjustifiably favor the state as a superuser or a user.

The third salient consideration that follows from the multiple functions of the state is agility. Cyber regulation must be flexible and adaptive in order to accommodate not only rapid transformations in technology,[212] the market, and society, but also changes in relationships between users, superusers, and the hosts of relevant regulators. As one agency, at the state or federal level, changes its regulatory approach, the polycentric characteristics outlined in this Article

208. *See generally* Claire A. Dunlop, Martino Maggetti, Claudio M. Radaelli & Duncan Russel, *The many uses of regulatory impact assessment: A meta-analysis of EU and UK cases*, 6 REG & GOVERNANCE 23 (2002).

209. For a discussion on secrecy in the context of cyber regulation, see Haber & Zarsky, *supra* note 190, at 570–72.

210. For more on oversight in this context, see Sarah Eskens, Ot van Daalen & Nico van Eijk, *Ten Standards for oversight and transparency of national intelligence services*, INSTITUTE FOR INFO. L. (2015), https://www.ivir.nl/new-ivir-report-on-oversight-on-intelligence-services/.

211. The U.S. experiment with FISA courts suggests that modifications may be required in order to ensure a genuine adversarial contest, and that a reasoned record (including judgments) is kept for ex post review. For more on the problems that arose in the FISA courts, see Elkin-Koren & Haber, *supra* note 42, at 154–56.

212. *See* Coldebella & White, *supra* note 67, at 241–42.

suggest that other segments of the matrix will be influenced. Similarly, as the state in its capacity of a superuser amends its *modus operandi*, some public entities in their roles as users could be affected, just as the change might affect all other users.[213]

This highlights the importance of continuously assessing what has changed, what works (or does not), and what may be the best response to these changes. Institutionally, that may entail having RIAs running constantly in the background, so as to provide decision-makers with a real-time picture of the challenges faced by the regulation of offense, defense, and surveillance as experienced by various regulators, public users, and superusers. Agility may also strengthen commitment to technology-neutral regulation, namely the commitment not to give regulatory preference to one technology over another, since such neutrality may prove useful in responding to ever-changing conditions, threats, and opportunities.[214]

This does not necessarily suggest that regulation should be amended on a daily basis. We usually associate regulation with some degree of rigidity, as there are costs associated with constant modification of regulation. Yet cyber stagnation in this respect could be dangerous when facing new threats, in part because the magnitude of ensuing damage from a regulatory failure may amount to a national disaster.[215] The potential volatility of the situation, therefore, requires that assessments regarding the costs and benefits of amending regulatory requirements be conducted in short intervals, and the regulation be modified only to the extent justified,.[216] Moreover, as this Article demonstrates, regulation is only one function performed by the state. It may act as a user and a superuser, and, therefore, policies regarding quick response by state entities (under attack, under surveillance, or when attacking) are of

213. Consider, for instance, how changes in the approach to net neutrality (treating all internet communications equally), whether by a regulatory agency like the FCC or by the state's power to shape it as a superuser, could affect other superusers and users alike. For more on net neutrality and regulation, see generally Lauren Gambino, *FCC flooded with comments before critical net neutrality vote*, THE GUARDIAN (Aug. 30, 2017), https://www.theguardian.com/technology/2017/aug/30/fcc-net-neutrality-vote-open-internet.

214. For more on the principle of technological neutrality, see, for example, Chris Reed, *Taking Sides on Technology Neutrality*, 4 SCRIPT-ED 263 (2007).

215. *See* Haber & Zarsky, *supra* note 190, at 560.

216. For instance, under its mission to strengthen private ICT providers, the government will "promote an adaptable, sustainable, and secure technology supply chain that supports security based on best practices and standards." *The National Cyber Strategy*, *supra* note 66, at 9. Furthermore, the Government "will convene stakeholders to devise cross-sector solutions to challenges at the network, device, and gateway layers, and . . . will encourage industry-driven certification regimes that ensure solutions can adapt in a rapidly evolving market and threat landscape." *Id.*

particular importance. In that respect, the state as a plural entity must be ready to actively react to new threats that may evade a slow-moving regulatory process. Such response policies are themselves a form of regulation, in the sense that when the state acts as a superuser, it indirectly affects the market. Therefore, the policies of state agencies—whether as superusers or as regulators—should be revisited on a continuous basis by looking not only at the emerging risks, but also at the realistic abilities of those subject to the regulation—including public bodies as users and state entities as superusers—to adapt quickly to amended regulation. In that respect, the term "responsive regulation," which usually refers to the capacity of a regulation to respond to concerns of the industry as well as to enforcement challenges,[217] gains another dimension. The state, or more specifically the multiple bodies that comprise the state, must respond to needs and actions by other state agencies, as well as to threats and vulnerabilities generated by other state bodies. Put differently, the response, so central to responsive regulation, is not merely the response to concerns of the industry or to threats generated by the industry, but also to regulation or to action by other state bodies. Moreover, such response may entail not only invoking regulatory power, but also resorting to the state's superuser capacity (i.e., response by market power or response by designing technology), and, in that sense, it is a form of indirect regulation. In turn, such response must also take into account the concerns of state entities as users, just like it must be sensitive to concerns of other, non-state users.

V. CONCLUSION

This Article unveiled three different roles occupied by the state in cyber: user, regulator, and superuser. These roles pull in different directions and generate conflicting pressures on the state, which arise from different interests, and thus could lead to suboptimal cyber regulation. The Article also documented the plurality of regulators in charge of addressing cyber defense, offense, and surveillance. Lastly, we argued for a regulatory approach that is collaborative (and thus both decentralized and coordinated), committed to oversight (as a matter of procedures, institutions, and culture), and agile (and thus requires ongoing evaluation, responsiveness, and adaptability).

On a deeper level, the plurality of the state corresponds with two conflicting images of state agencies in cyber. One is of the state as a clunky, bureaucratic, slow, and inefficient entity, likely to err either in identifying the goals for its intervention or in enlisting the optimal means for achieving them

217. *See generally* Robert Baldwin & Julia Black*, Really Responsive Risk-Based Regulation*, 32 L. & POL'Y 181 (2010) (explaining responsive regulation).

(or both) because it is too weak. The opposing image is that of the state as a tough, muscular, and highly powerful entity—a Leviathan—likely to overkill. While these two images seem to conflict, they appear to generate a similar attitude in favor of curbing the role of the state. Under the first vision of the state as a disorganized gaggle of clumsy agencies, minimizing its role is preferable because the state will likely underperform (at the taxpayers' expense), by standing in the way of progress and innovation. Under the second vision of the state as the Incredible Hulk, keeping the state's role limited is advisable because it can overperform and, in so doing, trample upon rights or otherwise disrupt delicate nuances better left to the market.

Yet these contradictory images of the state obscure the possibility that, while both may be right in certain respects, both may point in the opposite direction, namely towards the recognition of the role the state plays (and should be playing). As a powerful body, the state's presence may be important, if not necessary, to curtail the misuse of power of other powerful entities (other superusers or states). In so doing, the state is essential for protecting users (including itself as a flock of users) from other users or superusers, since trusting the market alone to generate the optimal level of cyber defense by trial-and-error entails significant risks. The price of errors can be overwhelming. Surely, as a powerful body, some checks and balances are required, and it may be the case that those developed with nineteenth century technologies in mind may prove insufficient.

As a clunky and less organized body, regulation might be needed precisely in order to align and coordinate governance. Such processes may not necessarily aim at generating a Leviathan, as the goal may instead be aimed towards bringing various entities to the table—regulators, users, and superusers—in order to facilitate information sharing and risk assessments. We do not think that one vision of the state should be preferred over the other, as both facets are true to an extent. Nor do we think that they cancel each other out. However, they are important to keep in mind, as this duality may inform one's approach to the institutional, procedural, and substantive questions regarding optimal ways to regulate privacy, cybersecurity, the import or export of dual-use cyber technologies, due process in the algorithmic era, or any other cyber-related field.