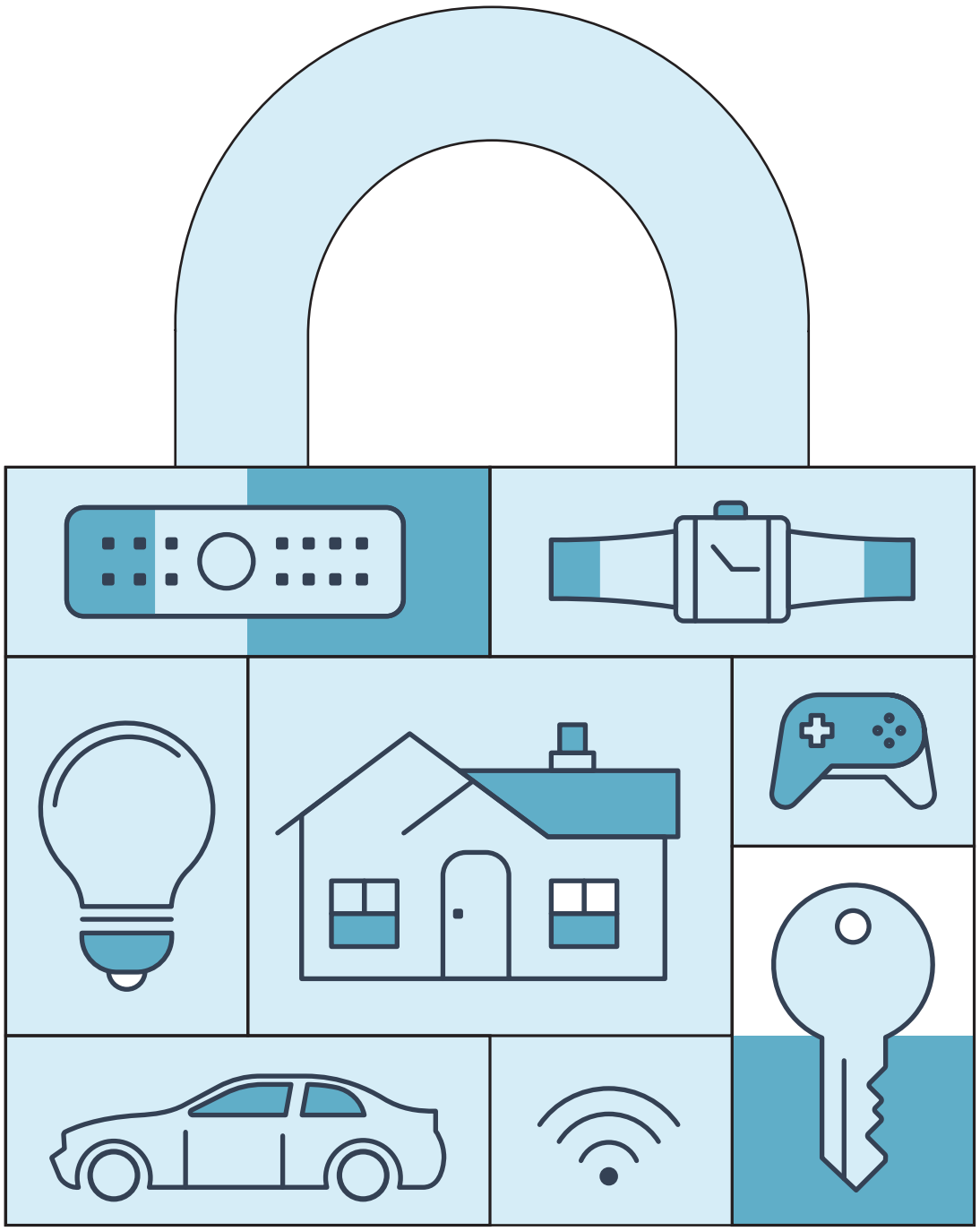

The Resilience Approach to Cybersecurity Policy in the Internet of Things Ecosystem

The Center for
Growth and **Opportunity**
at Utah State University

The Resilience Approach to Cybersecurity Policy in the Internet of Things Ecosystem

Author:
Anne Hobson[a]

July 2019
Policy Paper 2019.004

The Center for Growth and Opportunity at Utah State University is a university-based academic research center that explores the scientific foundations of the interaction between individuals, business, and government.

We support research that explores a variety of topics from diverse perspectives. Policy papers are published to stimulate timely discussion on topics of central importance in economic policy and provide more accessible analysis of public policy issues.

[a] Program Manager, Mercatus Center at George Mason University

The Center for Growth and Opportunity at Utah State University

Contents

Abstract **1**
I. Introduction **2**
II. IoT Governance Challenge **4**
III. Tension between Resilience and Security as Policy Goals **5**
IV. Resilience Approach **6**
A. Polycentricity 8
B. Peer-to-Peer Governance 10
C. Soft Law 11
D. Alternative Governance Projects in Action 11
V. Role of Risk, Uncertainty, and Learning **14**
VI. Conclusion **16**

Abstract

The Internet of Things includes consumer devices as well as the United States' critical internet-enabled infrastructure. As the planet-wide usage of internet-enabled devices passes the threshold of one device per person, the number of threat vectors and vulnerabilities is also increasing. However, cyber insecurity is increasingly viewed as a market failure in need of a comprehensive legislative solution at the federal and state levels. Nevertheless, the uncertainty and dynamism of the IoT ecosystem limits the effectiveness of ex-ante policy guidance. This paper argues that device insecurity requires solutions from a variety of stakeholders and alternative sources of governance. The resilience approach recognizes that the only sustainable way to confront large-scale disturbances is to empower stakeholders at multiple levels to remain persistent in the face of threats. The resilience approach requires a paradigm shift that encourages members of the IoT ecosystem to embrace risk and uncertainty and to learn by experience.

I. Introduction

Traditional connected devices are on the decline. Laptop and desktop computers now account for less than 25 percent of internet network traffic. In their place, the network of connected devices that send and receive data is set to expand massively. Known as the Internet of Things (IoT), this array of devices includes everything from smartphones to connected cars to critical infrastructure.[1] The IoT is an ecosystem that results from an iterative process of interaction between individuals—from the purchase of connected devices at the user level to the implementation new security processes at the developer level. Individuals participating in the IoT ecosystem include end users, cybersecurity researchers, security professionals, device manufacturers, developers, social entrepreneurs, and members of formal and informal governing bodies whose activities contribute to cybersecurity outcomes.

The quantity of IoT-capable devices surpassed two devices per person on the planet in 2018, amounting to 17 billion unique devices.[2] Worldwide, the number of IoT devices aside from smartphones, tablets, and laptops recently outstripped the number of mobile phones.[3] The IoT market is expected to more than double, to $520 billion, between 2017 and 2021. The fastest-growing subsector is data centers and analytics.[4] IoT products related to manufacturing, connected cars, transportation, and logistics will also drive growth.[5]

Cyberattacks are also increasing in scale and frequency. In 2014, a Chinese national helped remove the records of approximately 21.5 million former and current US government employees in a hack on the US Office of Personnel Management.[6] In 2016 , Yahoo reported the two largest data breaches to date, affecting 3 billion users.[7] In the same year, the Mirai botnet infected more than 600,000 devices and disrupted high-profile websites such as Twitter and Netflix.[8] Ransomware, distributed denial-of-service attacks, and data breaches demonstrate the challenge of data security.

In response, policy makers are pursuing formal laws and regulations to address cyber insecurity and related data privacy concerns. For example, the European Union's General Data Protection Regulation (GDPR) went into effect in May 2018. The GDPR requires that businesses that handle personal data use the highest possible privacy settings by default, allow data portability, disclose any data collection, and explain their data retention and third-party access policies. The GDPR includes fines for businesses that fail to report data breaches within 72 hours.[9] The international association of privacy professionals found that "the average organization spent $3 million dollars on [GDPR] compliance efforts" and estimated that it takes an "average of seven months to complete the requirements." The expected timeline for large companies is much longer.[10]

In the US, proposed federal legislation such as the Consumer Data Protection Act, the Data Care Act, and the American Data Dissemination Act would broaden the regulatory powers of the Federal Trade

1 Hobson 2017.
2 Knud Lasse Lueth, "State of the IoT 2018: Number of IoT Devices Now at 7B—Market Accelerating," IoT Analytics, August 8, 2018, https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/.
3 Lueth, "State of the IoT 2018."
4 Ann Bosche et al., "Unlocking Opportunities in the Internet of Things," Bain & Company, August 7, 2018, https://www.bain.com/insights/unlocking-opportunities-in-the-internet-of-things/.
5 Deloitte and Confederation of Indian Industry, "Harnessing the Power of Internet of Things to Transform Industry in India," 2018, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/manufacturing/in-mfg-harnessing-the-power-noexp.pdf.
6 Brian Krebs, "Congressional Report Slams OPM on Data Breach," *Krebs on Security*, September 7, 2016, https://krebsonsecurity.com/tag/opm-breach/.
7 Selena Larson, "Every Single Yahoo Account Was Hacked—3 Billion in All," *CNN Business*, October 4, 2017, https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html. (Larson 2017)
8 Anne Hobson, "Aligning Cybersecurity Incentives in an Interconnected World" (R Street Policy Study No. 86, February 2017).
9 EU General Data Protection Regulation (GDPR), Regulation (EU) 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 movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119/1).
10 International Association of Privacy Professionals and Ernst & Young Global Limited, "IAPP-EY Annual Privacy Governance Report 2018," 2018, https://www.ey.com/Publication/vwLUAssets/ey-iapp-ey-annual-privacy-gov-report-2018/$File/ey-iapp-ey-annual-privacy-gov-report-2018.pdf.

Commission (FTC) and thereby challenge the existing model of light-touch regulation.[11] For example, the Consumer Data protection Act calls for the establishment of a new Bureau of Technology within the FTC and would expand the definition of harm from data breaches to include noneconomic injury. At the state level, California passed the California Consumer Privacy Act (CCPA) of 2018 as well as a separate bill that requires "reasonable security features" for connected devices.[12] Similar to the GDPR, the CCPA introduces civil penalties and requires companies to disclose data practices, remove data when users request its removal, and permit users to opt out of data collection. Both laws go into effect in 2020. Hawaii and New Mexico are also considering broad privacy legislation modeled on the CCPA. The proposed bipartisan Cybersecurity Improvement Act of 2019 requires that devices purchased by the government comply with baseline security requirements developed by National Institute of Standards and Technology.[13]

In stark contrast to this new wave of legislative efforts, historically, the US approach has been light-touch. The federal government addresses harm on a case-by-case basis and relies on ex-post enforcement by the FTC to deal with data breaches and privacy concerns. Such ex-post enforcement can ensure that there is a sufficiently high cost to cybersecurity failures that result in tangible harm. For example, the FTC filed a claim against D-Link for releasing IoT products, including a connected baby monitor, with known vulnerabilities despite advertising that the products were secure.[14] Compared to the GDPR, which constrains wide swaths of data practices, the US approach is permissive to the risk-taking and trial and error necessary for innovation.

New legislative efforts are concerning because design requirements and processes can encourage compliance rather than security. To cite a historical example, it is believed that new requirements resulting from the Three Mile Island partial meltdown of a nuclear reactor drew manpower from routine inspections and may have contributed to the accident at Indian Point the following year.[15] Furthermore, requirements can become outdated and stunt the experimentation necessary to address emerging threats.[16] Wildavsky finds that "the conscientious effort of regulators to follow a prescriptive safety regime conflicts with their need to be responsive to current safety concerns."[17] If increasing security measures does not linearly increase security, and may in fact impair security outcomes, then what can policy makers do to secure the IoT?

This paper outlines a resilient policy approach to addressing cyber threats. Resilience can be best defined as " the ability to prepare and plan for, absorb, recover from or more successfully adapt to actual or potential adverse events."[18] The goal of this paper is twofold. First, it will demonstrate the complexity and dynamism of the digital ecosystem and the resulting policy challenge, including the tension between viewing security as a process and viewing it as an end goal for policy. Second, this paper will provide an alternative framework for thinking about how to address cyber insecurity.

Achieving resilience from cyberattacks requires an approach that acknowledges the complexity of designing policies to mitigate cyber insecurity. Allowing organizations to develop the capacity for resilience will

11 Jennifer Huddleston, "An Analysis of Recent Federal Data Privacy Legislation Proposals" (Policy Brief, Mercatus Center at George Mason University, March 2019).
12 2018 Cal. Legis. Serv. Ch. 886 (S.B. 327) (to be codified at Cal. Civ. Code § 1798.91.04). See also Gibson, Dunn & Crutcher, "New California Security of Connected Devices Law and CCPA Amendments," October 5, 2018, https://www.gibsondunn.com/new-california-security-of-connected-devices-law-and-ccpa-amendments/.
13 Senator Mark R. Warner's office, "Bipartisan Legislation to Improve Cybersecurity of Internet-of-Things Devices Introduced in Senate & House," press release, March 11, 2019, https://www.warner.senate.gov/public/index.cfm/2019/3/bipartisan-legislation-to-improve-cybersecurity-of-internet-of-things-devices-introduced-in-senate-house.
14 Federal Trade Commission, "D-Link Case Alleges Inadequate Internet of Things Security Practices," press release, January 5, 2017.
15 Wildavsky 1988, 139.
16 Anne Hobson, "Should the Government Require Companies to Meet Cybersecurity Standards for Critical Infrastructure?," *Wall Street Journal*, November 12, 2018, https://www.wsj.com/articles/should-the-government-require-companies-to-meet-cybersecurity-standards-for-critical-infrastructure-1542041617.
17 Wildavsky 1988, 146.
18 National Research Council, *Building Community Disaster Resilience through Public-Private Collaboration* (Washington, DC: National Academic Press, 2001).

require informal governance mechanisms [19] and efforts from a variety of stakeholders, including policy makers, end users, internet service providers, civil society, national standards bodies, and cybersecurity researchers. The resilience approach will require a flexible policy environment that allows for the development of public and private solutions ranging from certification programs and information-sharing efforts to cyber-insurance adoption and the promulgation of industry best practices. An approach that allows stakeholders to contribute to governance is most suited to addressing the complexity and dynamism of evolving threats in the IoT ecosystem.

II. IoT Governance Challenge

We rely increasingly on connected devices to cooperate, communicate, and exchange with one another. Adults in the US spend on average 11 hours and 6 minutes, or nearly half a day, interacting with digital media.[20] Increasingly, objects from cars to thermostats are connected to the internet, multiplying the number of potential threat vectors for data breaches and further complicating the IoT environment. Securing the IoT is a collective action problem in that the actions and cooperation of many stakeholders are required to address the changing landscape. Complexity can be a feature, not a bug, if individuals embrace a governance approach that takes it into account.

The IoT ecosystem is similar to some ascendant views of the market in that it is "an ecological system that emerges out of cultural and biological evolutionary processes."[21] By contrast, the static, mechanical views the state of cybersecurity in the IoT as the result of a market failure that has already emerged. For example, the Center for Democracy & Technology finds that cyber insecurity is due to information asymmetry between buyers and sellers of IoT devices, negative externalities in the form of botnet- or malware-related disruptions not necessarily borne by the owners of the devices, and moral hazard in that consumers bear the costs of the risky actions of device manufacturers.[22] Furthermore, security technologist Bruce Schneier argues that "the economics of the IoT mean that it will remain unsecure unless government steps in to fix the problem. . . . This is a market failure that can't get fixed on its own."[23]

Even if insecurity is the IoT's dominant state at one point, the static view assumes that the ecosystem will necessarily remain insecure absent regulatory intervention in the form of the top-down introduction of strict products liability, the implementation of a minimum security standard, or the tasking of a government agency to enforce cybersecurity.[24] When the state is "elevated to the status of the main tool for collective action or instrument for any conceivable policy solution, . . . any alternative form of organization or conceptualization was either considered irrelevant or marginalized."[25] The belief in the state as the sole source of governance capable of addressing insecurity ignores the fact that the IoT ecosystem is constantly changing and solutions are emerging. The static view also downplays the role of imaginative individuals in finding opportunities to create value—whether this takes the form of the provision of cyber insurance, an IoT device certification program, or the invention of cheaper methods of detecting malware.

19 For the purposes of this paper, *governance* is defined as a process of interaction among decision-makers that leads to informal or formal rules that constrain behavior. While government is recognized as providing formal governance, any organization or individual involved in the process of forming rules is producing, and often coproducing, governance.

20 Nielsen, "Time Flies: US Adults Now Spend Nearly Half a Day Interacting with Media," July 31, 2018, https://www.nielsen.com/us/en/insights/news/2018/time-flies-us-adults-now-spend-nearly-half-a-day-interacting-with-media.html.

21 Vernon L. Smith, "Constructivist and Ecological Rationality in Economics," *American Economic Review* 93, no. 3 (2003): 465–508.

22 Benjamin C. Dean, "An Exploration of Strict Products Liability and the Internet of Things," Center for Democracy & Technology, 2018.

23 Bruce Schneier, "We Need Stronger Cybersecurity Laws for the Internet of Things," *CNN Opinion*, November 10, 2018, https://www.cnn.com/2018/11/09/opinions/cybersecurity-laws-internet-of-things-schneier/index.html.

24 Notably, agencies are already tasked with enforcing cybersecurity in a variety of contexts. Researchers Eli Dourado and Andrea O'Sullivan found that in 2015, at least 62 federal offices were tasked with significant cybersecurity priorities, many with nearly identical mission statements. The Government Accountability Office found that unclear responsibilities in federal cybersecurity limited the effectiveness of these offices. Eli Dourado and Andrea O'Sullivan, "Dozens of Federal Cybersecurity Offices Duplicate Efforts with Poor Coordination," Mercatus Center at George Mason University, April 14, 2015.

25 Paul D. Aligica and Peter J. Boettke, *Challenging Institutional Analysis and Development: The Bloomington School* (New York: Routledge, 2009), 139.

Because the IoT is an ecosystem driven by change and interaction, it is necessarily dynamic. Cybersecurity is a moving target: there is no simple solution to cyber insecurity. Systems based on human activity "are messy and complex, and they operate in ways that are less than perfectly efficient—they are in a state of constant dynamic disequilibrium."[26] Surprises and uncertainty are guaranteed as the level of security changes through time. By contrast, the static and mechanical view assumes that insecurity is a technical problem that can be solved at a single moment in time. The static view treats the ecosystems in which human actors reside as predictable and controllable. As a result, the static view has fostered an analytical focus that treats cybersecurity as a market failure requiring government correction rather than as a collective action problem with a variety of possible solutions coming from stakeholders inside and outside government. Economist Elinor Ostrom emphasized the importance of dynamic experimentation among stakeholders:

> Instead of assuming that designing effective governance systems is a relatively simple analytical task that can be undertaken by a team of objective analysts sitting in the national capital, or at an international headquarters, it is important that we understand policy design to require experimentation with combinations of large numbers of component parts.[27]

Viewing a problem with a common pool resource—such as the internet—as a pervasive market failure leads to demands that a central power fix it.[28] However, those in favor of government regulation often don't consider that the regulatory requirements prescribed will have to adapt to evolving threats or changes in the polycentric map as new solutions or sources of governance emerge. The polycentric map, which will be discussed in detail in section 4, refers to the multiple, competing decision-makers or stakeholders in the IoT ecosystem. Furthermore, security can decay as "products and practices that were once helpful become harmful under altered circumstances," [29] moving resources toward compliance with regulations and away from securing against new threats.

Stakeholders need to shift away from viewing cybersecurity as a static, mechanical problem and toward viewing it as a dynamic, emergent problem. Reframing the role of policy makers as to foster the creation of a policy environment that allows solutions to arise will lead to a more resilient IoT ecosystem. As section 4 will explore, treating the IoT as a dynamic ecosystem has implications for the types of governance solutions policy makers pursue.

III. Tension between Resilience and Security as Policy Goals

There is a tension between an approach characterized by resilience and the government-led approach of comprehensive legislation that tasks agencies with ensuring commercial cybersecurity. Regulators face internal and external pressures to act in the name of safety by adding more device requirements, reviews, or procedures, whether or not those improve security outcomes.[30] When policy aims at the prevention of harm, it may, in fact, cause harm by getting the prescription wrong:

> The requirements of a policy of prevention are severe. One must judge which evils are likely to manifest themselves. Predicting wrongly, when these "guesstimates" are backed up by the force of the state, wreaks havoc upon innocents: lives are disrupted,

26 Andrew Zolli and Ann Marie Healy, *Resilience: Why Things Bounce Back* (New York: Free Press, 2012), 17.
27 Aligica and Boettke, *Challenging Institutional Analysis*, 155–56.
28 Aligica and Boettke, 149–50.
29 Wildavsky 1988, 227.
30 Wildavsky, 138.

> jobs lost, anxiety increased, and resources diverted from more productive and hence safer uses.[31]

In fact, making security the end goal may be deleterious: "A state of security may be dangerous in the long run . . . since it reduces the capacity to cope with unexpected hazards."[32] Furthermore, creating a false sense of security, as device requirements can do, compromises coping ability.[33]

When device security is viewed as an attainable end goal, the focus is on anticipation of harm and ex-ante avoidance of risk. Security is viewed as a technical problem with an attainable solution. Government need only require device manufacturers to implement that solution. However, as the previous section notes, the static view ignores the complexity and dynamism of the IoT ecosystem. Security is not a static problem; it is a moving target—an unknown to be continuously sought after. Because security is an elusive target and the methods by which to achieve it are unknown, the emphasis should be on the act of searching for ways to achieve device security.[34]

Because security is an unknown, making resilience the end goal is the preferable strategy . "The more widespread the search [for security], the more varied the probes and reactions, the more diverse the evaluating minds, positive and negative, the better. This method should be variegated—decentralized participatory , and based on diverse, repeated probes."[35] Applying Wildavsky's insights to the IoT ecosystem, multiple stakeholders—from agencies like the National Institute of Standards and Technology to device manufacturers and private cybersecurity providers—need to engage in trial and error to discover solutions to prepare for the unexpected cyberattack. In the dynamic view, cybersecurity is a process, not a goal to be aimed at and achieved by a single policy actor or action.

Both informal and formal institutions need to be involved in the governance process. In fact, these are two sides of the same governance coin: "Formal order, to be more explicit, is always and to some considerable degree parasitic on informal processes, which the formal scheme does not recognize, without which it could not exist, and which it alone cannot create or maintain."[36] Informal order includes social norms or customs that shape behavior, whereas formal order includes written laws and policies. As the next section will show, informal order is required for the IoT ecosystem to become resilient.

IV. Resilience Approach

An IoT ecosystem that is impervious to cyberattacks is unachievable. Instead, policy makers should aim for a system that is robust or resilient to attacks. In short, complex and unpredictable systems shouldn't be treated as simple, predictable systems. Instead, risk can be managed by fostering resilience. The resilience approach moves beyond short-term responses for specific incidents to longer-term, ecosystem-wide engagement with a variety of public and private efforts.

Achieving resilience means "preserving adaptive capacity—the ability to adapt to changed circumstances while fulfilling one's core purpose—and it's an essential skill in an age of unforeseeable disruption and volatility."[37] Andrew Zolli and Ann Marie Healy argue that

> enhancing the resilience of an ecosystem . . . can be achieved in two ways: by improving its ability to resist being pushed past these kinds of critical, sometimes

31 Wildavsky, 100.
32 Wildavsky, 87.
33 Wildavsky, 91; Hobson, "Should the Government Require Companies to Meet Cybersecurity Standards?"
34 Wildavsky 1988.
35 Wildavsky, 103.
36 James C. Scott, *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed* (New Haven, CT: Yale University Press, 1998), 310.
37 Zolli and Healy, *Resilience*, 7–8.

> permanently damaging thresholds, and by reserving and expanding the range of niches to which a system can healthily adapt if it is pushed past such thresholds.[38]

In the context of commercial cybersecurity, permanently damaging thresholds include the damage and destruction of critical infrastructure and economic losses because of cyberattacks that lead to bankruptcy.

Policies should make resilience the end goal. There are examples of US policy makers embracing the resilience approach, particularly in addressing the issue of automated distributed threats such as botnets. For example, the National Institute of Standards and Technology hosted a public workshop titled "Enhancing Resilience of the Internet and Communications Ecosystem."[39] In the resilience approach, the proper role of government is to foster resilience in a bottom-up fashion by supporting the digital ecosystem's own ability to adapt, recover, and rebuild in the face of cyberattacks. The resilience approach promotes efforts to "redesign our institutions, embolden our communities, encourage innovation and experimentation, and support our people in ways that will help them be prepared and cope with surprises and disruptions."[40]

Refraining from concentrating authority in rule-bound federal agencies by empowering other stakeholders is important. Alternative governance approaches that rely on peer production, informal norms, nonbinding standards, and multistakeholder efforts (explored in the following section) are best suited to adapt to the changing threat landscape. Achieving resilience requires supporting diverse, on-the-ground efforts:

> Such [resilient] systems embrace an ethic of decentralization and shared control—swarming—so that no single entity is absolutely in charge. But neither are they utterly anarchic. They do not do away with all centralized authority, but instead balance it with the right kinds of local empowerment and self-sufficiency.[41]

The resilience approach promotes entrepreneurship and requires that individuals within the ecosystem have the alertness, flexibility, adaptability, authority, and space to act independently and innovatively.

There is an element of messiness to a decentralized approach. However, humans have a long history of "muddling through," which emphasizes trials and errors, revisions, piecemeal improvements, and "disjointed incrementalism."[42] Sociologist James Scott argues that this messy approach "was meant to capture the spirit of a practical approach to large-scale policy problems that could not be completely understood, let alone comprehensively addressed."[43] A governance arrangement that operates as a network of decentralized, self-coordinating parts is best able to mitigate risk in a complex, dynamic environment. For the IoT ecosystem, Adam Thierer argues,

> the better alternative to top-down regulation is to deal with concerns creatively as they develop, using a combination of educational efforts, technological empowerment tools, social norms, public and watchdog pressure, industry best practices and self-regulation, transparency, and targeted enforcement of existing legal standards (especially torts), as needed.[44]

The subsections that follow further examine polycentric institutional arrangements such as peer-to-peer governance and soft law as alternatives to a centralized, top-down policy response to cyber insecurity.

38 Zolli and Healy, 8.
39 National Institute of Standards and Technology, "Enhancing Resilience of the Internet and Communications Ecosystem" (public workshop, National Cybersecurity Center of Excellence, Rockville, MD, July 11–12, 2017), https://www.nist.gov/news-events/events/2017/07/enhancing-resilience-internet-and-communications-ecosystem.
40 Zolli and Healy, *Resilience*, 23.
41 Zolli and Healy, 92.
42 Charles E. Lindblom, "Still Muddling, Not Yet Through," *Public Administration Review* 39 (1979): 517–26.
43 Scott, *Seeing Like a State*, 328.
44 Adam D. Thierer, "The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation," *Richmond Journal of Law and Technology* 21, no. 6 (2015): 4.

A. Polycentricity

Polycentricity refers to a governance environment where there are multiple, overlapping centers of decision-making, an approach pioneered by Michael Polanyi in 1951 and applied by Elinor Ostrom in her 1990 study of metropolitan governance and common pool resource management.[45] Before Ostrom especially, the consensus in public administration literature was that for public goods—including parks, defense, watersheds, and the internet—a tragedy of the commons would necessarily occur. However, Ostrom's empirical research pointed out the flaws in reliance on the tragedy-of-the-commons model:

> Many researchers drawing on these models have concluded that the participants in a commons dilemma are trapped in an inexorable process from which they cannot extract themselves. . . . Contemporary policy analysts also share the belief that it is possible to design and impose optimal rules for the management of common-pool resources from the top down. Because common pool resources, and their users, are viewed as relatively similar to one another, and because of the simplicity of the models, officials (assumed to be acting in the public interest) are thought to be capable of devising uniform and effective rules for an entire region.[46]

In the tragedy-of-the-commons model, farmers, households, and businesses are expected to siphon off the common resource for their individual use at the expense of the long-term sustainability of the resource, resulting in a market failure. Ostrom explains how the presumption of a market failure leads to calls for state intervention:

> The existing theory of collective action, which underlies the work of all political economists, has accentuated the presumed necessity of the State as an alternative to the Market, since the accepted theory predicts that voluntary self-organization to provide public goods or manage common-pool resources is highly unlikely.[47]

Ostrom detailed in countless examples how we observe individuals muddling through with alternative governance solutions for common pool resources, including social norms, associations, and sanctioning. Ostrom's examples include irrigation systems in Spain, the Philippines, and the US, as well as mountain grazing and forest management in Switzerland and Japan. In environments characterized by uncertainty, she finds that commitment and monitoring, operational rules that developed over time. [48] For example, in Swiss alpine meadows, local associations prevent overgrazing by allocating access rights to the meadow in different seasons on the basis of the number of animals that can be fed, the amount and value of the land owned, the amount of hay produced, and the number of shares individual users own in the cooperative. A lottery system is used to allocate timber rights.[49] In Spain, irrigation institutions developed over a millennium. Locally elected delegates make decisions about maintenance, and farmers take turns drawing water from the canal and monitor each other. In times of drought, norms have developed such that farmers take shorter turns and cheaters are punished with fines and humiliation.[50] In Ostrom's mind, overlapping governance efforts—as well as the variety and redundancy of efforts—are features of a resilient ecosystem:

> The strength of polycentric governance systems is that each of the subunits has considerable autonomy to experiment with diverse rules for a particular type of resource system and with different response capabilities to external shock. In experimenting with rule combinations within the smaller-scale units of a polycentric system, citizens and officials have access to local knowledge, obtain raid feedback

45 Michael Polanyi, *The Logic of Liberty* (Indianapolis, IN: Liberty Fund, 1951); Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (Cambridge: Cambridge University Press, 1990).
46 Aligica and Boettke, *Challenging Institutional Analysis*, 151–52.
47 Aligica and Boettke, 149–50.
48 Ostrom, *Governing the Commons*.
49 Ostrom, 64–65.
50 Ostrom, 73.

> from their own policy changes, and can learn from the experience of other parallel units. Instead of being a major detriment to system performance, redundancy builds in considerable capabilities. [51]

Ostrom identified several common traits for successful governance of common pool resources: defined boundaries for resource use; the inclusion of users in rule creation, monitoring, conflict-resolution mechanisms, and graduated sanctions; and polycentric order, among others.[52] She emphasized the importance of coordination through overlapping interorganizational arrangements that are capable of contributing to decision-making autonomously.

Ostrom's research recognized that we live in a complex, dynamic world with a multiplicity of actors. Government is just one actor in the IoT ecosystem, and companies, trade associations, civil society, and cybersecurity researchers all play a role in enhancing cybersecurity. In contrast to formal rules decreed from above, a polycentric system of governance should include a variety of institutional arrangements at multiple levels competing and cooperating in overlapping jurisdictions. The polycentric approach empowers IoT device users, who help set norms of behavior and thus have a say in the rule-making process.

Christopher Koopman and Matthew Mitchell explore the governance of the taxi industry as an example of polycentric order. They find that overlapping governance mechanisms—from state departments of motor vehicles and taxi commissions to the terms and conditions of taxi services and norms surrounding tipping, ratings, and reviews—permit agents within the system to opt in and out of institutional arrangements depending on the agents' changing needs and circumstances.[53] Polycentric systems are unique in that they are capable of spontaneous self-correction: "A political system that has multiple centers of power at differing scales provides more opportunity for citizens and their officials to innovate and to intervene so as to correct maldistributions of authority and outcomes."[54]

The polycentric governance approach parallels the existing governance structure of the internet. The Clinton administration's 1997 Framework for Global Electronic Commerce deliberately carved out space for e-commerce to flourish. The US follows this framework by default. Milton Mueller offers a comprehensive analysis of network actors outside the nation-state system as well as of their effectiveness in addressing cybersecurity issues.[55] Such large international organizations as Internet Corporation for Assigned Names and Numbers (ICANN), the World Intellectual Property Organization (WIPO), and Internet Governance Forum (IGF) are forums for developing governance solutions at the international level. Mueller argues that more efficient institutions and new organizational forms are in a continuous process of emerging out of the interactions between public and private actors. He proposes that a "denationalized liberal approach" that emphasizes cooperation between stakeholders is the best approach for internet governance. The tenets of "polycentricity" and "decentralized liberalism" capture the wisdom of distributed networks of decision-making. Multistakeholder efforts, in which individuals or organizations interested in a common goal participate in dialogue and the development of solutions, have long been documented for their capacity to enhance organizational learning and support decentralized decision-making.[56] Notably, not all multistakeholder orders are polycentric: polycentricity depends on the distribution of authority and decision-making power among actors. In a polycentric order, overlapping authority between different actors injects competition into the institutional arrangement.

It is also important to note that the imposition of a uniform, static approach to cybersecurity policy at the state or federal level does not mean that polycentric behavior comes to a full stop. Regardless of the policy

51 Aligica and Boettke, *Challenging Institutional Analysis*, 157.
52 Ostrom, *Governing the Commons*.
53 Matthew Mitchell and Christopher Koopman, "Taxis, *Taxis* and Governance in the Vehicles-for-Hire Industry" (Working Paper 2018.002, Center for Growth and Opportunity at Utah State University, June 2018), https://www.growthopportunity.org/research/working-papers/taxis-taxis-and-governance-in-the-vehicles-for-hire-industry/.
54 Paul D. Aligica and Vlad Tarko, "Polycentricity: From Polanyi to Ostrom, and Beyond," *Governance* 25 (2012): 245.
55 Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: MIT Press, 2013).
56 Mueller, *Networks and States*.

environment, the decentralized and evolving nature of the IoT would still mean that polycentric processes would take place and solutions would emerge. Furthermore, static approaches can morph over time to make space for polycentric behavior. Even if regulators freeze a set of baseline design requirements in place, the existing organizational apparatus, from company security teams to cyber insurers to civil society, does not dissolve overnight. Individuals will still experiment and the demand for new approaches will increase over time. This means that, regardless of the path of policy in the US, adaptability and resilience are still achievable goals. However, the polycentric-permissive approach would facilitate a resilient ecosystem more quickly and result in fewer resources being misallocated to compliance and rent-seeking.

The polycentric approach incorporates ideas about open-endedness and evolution consistent with Abigail Devereaux and Richard Wagner's framing of the appropriate vision for a complex social system.[57] Placing polycentric ends in the analytical foreground shifts the government's role from forcibly fixing a static problem to fostering an ecosystem in which governmental and nongovernmental organizations and institutional arrangements emerge through interaction. Instead of focusing on designing optimal rules, a polycentric approach emphasizes developing an optimal, resilient environment through which rules will emerge.

> Polycentric systems are themselves complex adaptive systems without one dominating central authority. Thus, no guarantee exists that such systems will find combinations of rules at diverse levels that are optimal for any particular environment. In fact, one should expect that all governance systems would be operating at less than optimal levels, given the immense difficulty of fine-tuning any complex, multi-tiered system. But because polycentric systems have overlapping units, information about that has worked will in one setting cane be transmitted to other units. And when small systems fail, there are larger systems to call upon—and vice versa.[58]

Christopher Coyne and Jayme Lemke argue that polycentric orders are the converse of top-down, monocentric orders in that polycentric orders capture local knowledge and afford flexibility in disaster response rather than rigidity.[59] Because a more polycentric approach leaves space for governance in a bottom-up fashion, it is more suited to address the complexity, uncertainty, and dynamism characteristic of the IoT ecosystem.

B. Peer-to-Peer Governance

Peer-to-peer governance is a movement in which groups that manage digital resources engage in experimentation at the firm and institutional level. Like polycentric order, it captures the spirit of decentralization, but with an emphasis on open-source processes of developing technologies. "Peer production" is a form of mass collaboration that grew up within the internet.[60]

Peer-to-peer governance relies on self-organizing communities of individuals to achieve an outcome. Products or solutions are crowdsourced and constitute peer production. Wikipedia's governance model is the most well known example of peer-to-peer governance. Peer production can include broader ends such as cybersecurity. Bug bounty programs (in which individuals can receive compensation for identifying exploits and vulnerabilities) and some forms of red-teaming (in which an independent group attempts to

57 Abigail Devereaux and Richard E. Wagner, "Contrasting Visions for Macroeconomic Theory: DSGE and OEE," *American Economist*, 2017. Graham Room also advocated for a complex-systems view of the world that takes into account the multilayered and multileveled policy landscape, the power and position of each stakeholder in society, and the feedback loops through which policy continuously develops. In Room's view, individuals are agile experimenters that transform and cocreate their policy environment. Graham Room, *Agile Actors on Complex Terrains: Transformative Realism and Public Policy* (New York: Routledge, 2016).
58 Aligica and Boettke, *Challenging Institutional Analysis*, 157.
59 Christopher J. Coyne and Jayme S. Lemke, "Polycentricity in Disaster Relief," *Studies in Emergent Orders* 4 (2011): 40–57.
60 Yochai Benkler, "Freedom in the Commons: Towards a Political Economy of Information," *Duke Law Journal* 52, no. 6 (2003): 1245.

improve security by assuming the role of an adversary) are forms of peer production and incite a process of iteration that improves the quality of output.

Criticism of peer production can also be applied to polycentricity and other forms of decentralized governance—these institutions can themselves require costly consensus processes, which can become paralyzing as the size of stakeholders involved increases. Moreover, because of peer production's reliance on informal processes, some scholars argue that the quality of the outcome is lower compared to a more bureaucratic approach.[61] Peer-to-peer governance provides another lens through which to understand institutional experimentation in the internet age.

C. Soft Law

Soft law is a set of informal norms, multistakeholder arrangements, and nonbinding (or soft) guidance standards that provide an adaptable alternative to regulation or legislation.[62] Soft law mechanisms include workshops such as the FTC's workshop on the IoT,[63] agency guidance such as the NIST Framework by the National Institute of Standards and Technology,[64] industry best practices and standards,[65] and other multistakeholder processes such as the National Telecommunications and Information Administration's workshop on software transparency for IoT products.[66] By emphasizing informal and flexible rulemaking from a variety of sources over formal administrative regulations from one source, soft law encourages resilience.

A soft law approach to emerging technologies allows for institutional trial and error, which leads to more robust and decentralized systems that are less vulnerable to cybersecurity threats. A cybersecurity ecosystem governed by soft law, peer production, or other polycentric orders will take the form of a "rich stew made up of bits and pieces of public and private organizations, informal social networks, government agencies, individuals, social innovators, and technology platforms, all working together in highly provisional, spontaneous, and self-organized ways."[67] From the diversity and redundancy of governance providers comes the resilience of the ecosystem as a whole.

D. Alternative Governance Projects in Action

Because of the complexity and dynamism of the IoT ecosystem, it is impossible to predict what form alternative governance arrangements will ultimately take. Indeed, "since each disruption and circumstance is unique, there can be no prefabricated organizational chart for the players."[68] Instead, "maintaining a redundancy of means and a varied repertoire of responses to unpleasant surprises" leads to the best security outcomes.[69] There have been attempts to characterize and map structures that entail the participation of multiple stakeholders; however, these observations are ex-post analyses of structures at a specific moment of time. James Scott notes that "any large social process or event will inevitably be far more complex than the schemata we can devise, prospectively or retrospectively, to map it."[70] Nevertheless, there are key players and efforts emerging that are consistent with the resilience approach.

61 Daniel Kreiss, Megan Finn, and Fred Turner, "The Limits of Peer Production: Some Reminders from Max Weber for the Network Society," *New Media & Society* 13, no. 2 (2010): 243–59.
62 Ryan Hagemann, Jennifer Skees, and Adam D. Thierer, "Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future," *Colorado Technology Law Journal* 17, no. 1 (2018): 37–130.
63 Federal Trade Commission, "The Internet of Things: Privacy and Security in a Connected World" (workshop, Washington, DC, 2015).
64 National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," January 10, 2017, https://www.nist.gov/sites/default/files/documents/draft-cybersecurity-framework-v1.11.pdf.
65 Institute of Electrical and Electronic Engineers, "IEEE-SA IoT Ecosystem Study," 2015, http://standards.ieee.org/innovate/iot/.
66 National Telecommunications and Information Administration, "NTIA Software Component Transparency" working group website, accessed July 24, 2019, https://www.ntia.doc.gov/SoftwareTransparency.
67 Zolli and Healy, *Resilience*, 264.
68 Zolli and Healy, 264.
69 Wildavsky 1988, 233.
70 Scott, *Seeing Like a State*, 309.

Presidential Policy Directive 8 in 2011 and Presidential Policy Directive 21 in 2013, as well as Executive Order No. 13,636, "Improving Critical Infrastructure Cybersecurity," tasked federal agencies with achieving resilience as a buffer against catastrophic events.[71] For example, Presidential Policy Directive 8 specifies the following goal for agencies: "a secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to and recover from the threats and hazards that pose the greatest risk."[72] The concept of the "whole community" includes individuals, families, businesses, community groups, nonprofit organizations, and representatives from all levels of government. However, efforts remain disjointed, with at least seven federal agencies[73] and departments producing resilience frameworks.[74] While existing frameworks still focus primarily on resilience in the physical domain rather than in the domain of people and processes, the emphasis is changing. The Department of Homeland Security announced a different approach to securing critical infrastructure that includes not just hardware and structures but also "people and physical and cyber systems that work together in processes that are highly interdependent."[75]

Empowering individuals is a critical aspect of a successful governance framework. Informal governance can take the form of reputational mechanisms such as ratings and reviews that help consumers steer clear of insecure products.[76] Journalists and cybersecurity researchers can draw consumer attention to errant companies. For example, as a result of public pressure, a Chinese company whose webcams were leveraged in the Mirai botnet chose to recall millions of devices.[77] Cyber hygiene education and public and private digital literacy efforts help arm IoT device users with beneficial information. Contests can also incentivize creative solutions. With the goal of securing vulnerabilities in home IoT devices, the FTC announced awards for contestants who could provide the best technical solution.[78] Social norms, such as password complexity and password management practices and proper responses to phishing emails, moderate behavior. IoT device users can also lead by example by actively prioritizing cybersecurity. Products such as smart firewalls or smart routers monitor connected devices and can tell users when their devices are infected with malware or are participating in a malicious botnet.

The use of guarantees and warranties by IoT device manufacturers or cybersecurity service providers builds trust by signaling that companies have invested in the security of their products. Device certification programs, such as UL's Cybersecurity Assurance Program and the Online Trust Alliance's 2017 "IoT Trust Framework," provide consumers with information about how well devices protect data.[79] More formal ex-post governance mechanisms include common-law remedies such as torts as well as case-by-case enforcement of antifraud statutes by the FTC and state attorneys general.

---

71 Presidential Policy Directive/PPD-8, "National Preparedness," White House, Washington, DC, March 30, 2011, https://www.dhs.gov/presidential-policy-directive-8-national-preparedness; Presidential Policy Directive/PPD-21, "Critical Infrastructure Security and Resilience," White House, Washington, DC, February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil; Exec. Order No. 13,636, 3 C.F.R. 217 (2014).

72 PPD-8, "National Preparedness."

73 Agencies and departments developing assessment frameworks for disaster resilience include the Department of Homeland Security, the Federal Emergency Management Agency, the Department of the Interior, the Environmental Protection Agency, the National Institute of Standards and Technology, the National Oceanic and Atmospheric Administration, the US Army Corps of Engineers, the US Army Environmental Command, the Department of Health and Human Services, the Department of Agriculture, the Department of Transportation, the General Services Administration, the Department of Commerce, and the Department of Energy.

74 Sabrina Larkin et al., "Benchmarking Agency and Organizational Practices in Resilience Decision Making," *Environmental System Decisions* 35, no. 2 (2015): 185–95.

75 US Department of Homeland Security, "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets," February 2003, https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf.

76 Adam D. Thierer et al., "How the Internet, the Sharing Economy, and Reputational Feedback Mechanisms Solve the 'Lemons Problem,'" *Miami Law Review* 70, no. 3 (2015).

77 Michael Mimoso, "Chinese Manufacturer Recalls IOT Gear Following Dyn DDoS," *Threat Post*, October 24, 2016, https://threatpost.com/chinese-manufacturer-recalls-iotgear-following-dyn-ddos/121496/.

78 Federal Trade Commission, "FTC Announces Internet of Things Challenge to Combat Security Vulnerabilities in Home Devices," press release, January 4, 2017.

79 UL, "Cybersecurity Assurance Program: First Standards-Based Internet of Things (IOT) Security Certification Program," accessed July 24, 2019, https://ctech.ul.com/en/services/cybersecurity/cybersecurity-assurance-program/; Online Trust Alliance, "IoT Security & Privacy Trust Framework v2.5," 2017, https://www.internetsociety.org/wp-content/uploads/2018/05/iot_trust_framework2.5a_EN.pdf.

Cyber insurance is a critical market-based mechanism that improves cybersecurity outcomes in the IoT.[80] Cyber insurance aligns the incentives of IoT companies with those of insurers through the underwriting process. During the underwriting process, insurers are incentivized to ensure that firms remain vigilant to threats. Manufacturers perform risk assessments and are incentivized to become aware of vulnerabilities and put basic cyber practices in place in order to obtain lower premiums. Basic cyber practices can include adopting industry best practices or voluntary standards such as the US government's NIST Framework for improving critical infrastructure cybersecurity.[81] Blockchains, as distributed ledgers, can also play a role in improving cybersecurity for internet-connected critical infrastructure by serving as transparent and trustworthy certificate authorities (the third parties that verify that companies and website owners are who they say they are).[82] Whether blockchains can aid in the public certification of IoT devices or be used to monitor the quality of their supply chains remains to be seen.

Increased cyber insurance adoption could bolster the IoT ecosystem as a whole. Increased adoption of baseline standards raises the bar for device security among the insured and uninsured.[83] In fact, insurers are sharing information to create a common assessment of cybersecurity software and technology to aid consumers in identifying quality services.[84] Voluntary frameworks and standards produced through multistakeholder processes such as the "internet security and upgradability and patching" working group, held in collaboration with industry and civil society, have helped further to fill the governance gap caused by the pacing problem.[85] The Institute of Electrical and Electronics Engineers contributed technical standards for the security of the IoT ecosystem for technologies such as Wi-Fi and Ethernet.[86]

When it comes to threat information-sharing and producing a fast system-wide response to a cyberattack, emergent multiorganization networks can help. Increasingly employed in the context of response to natural disasters, these networks allow a variety of organizations to interact with formal state and federal agencies to tackle a specific problem.[87] There have been other promising developments in collaboration between the private and public sectors. Benoit Dupont documents two examples of emergent polycentric approaches—civil remedies and regulatory strategies—that rely on public-private coordination to disrupt malicious botnets and help infected victims recover their computer equipment.[88] USTelecom and the Information Technology Industry Council in 2018 announced the creation of a Council to Secure the Digital Economy to drive cyber solutions. For example, the new council created a botnet guide that can be implemented in a variety of industries to mitigate IoT-related distributed denial of service attacks. Cybersecurity guarantees, certifications, and ratings; cyber-insurance adoption; and the adoption of industry best practices are examples of governance that show that multistakeholder arrangements can achieve sustainable long-term management of a shared resource such as the IoT.

In a complex ecosystem, it is important that "rules emerge as a spontaneous order—they are found—not deliberately designed by one calculating mind."[89] The process of rule emergence is in a constant state of unfolding in the IoT ecosystem:

80 Hobson, "Aligning Cybersecurity Incentives."
81 National Institute of Standards and Technology, "Framework."
82 Scott J. Shackelford and Steve Myers, "Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace" (White Paper Series, Ostrom Workshop, Program on Cybersecurity and Internet Governance, 2017).
83 Anne Hobson, "Comments of the R Street Institute," In the Matter of the Request for Comments on the 2017 Draft Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, Before the National Institute of Standards and Technology, Washington, DC, April 10, 2017, https://www.nist.gov/sites/default/files/documents/2017/04/19/2017-04-10_-_r_street_institute.pdf.
84 Leslie Scism, "Insurers Creating a Consumer Ratings Service for Cybersecurity Industry," *Wall Street Journal*, March 26, 2019, https://www.wsj.com/articles/insurers-creating-a-consumer-ratings-service-for-cybersecurity-industry-11553592600.
85 National Telecommunications and Information Administration, "Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching," working group website, accessed July 24, 2019, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.
86 Institute of Electrical and Electronic Engineers, "IEEE-SA IoT Ecosystem Study."
87 Danielle M. Varda et al., "Social Network Methodology in the Study of Disasters: Issues and Insights Prompted by Post-Katrina Research," *Population Research and Policy Review* 28, no. 1 (2009): 11–29.
88 Benoit Dupont, "Bots, Cops and Corporations: On the Limits of Enforcement and the Promise of Polycentric Regulation as a Way to Control Large-Scale Cybercrime," *Crime, Law and Social Change*, 2016.
89 Smith, "Constructivist and Ecological Rationality," 324.

> Initially constructivist institutions undergo evolutionary change adapting beyond the circumstances that gave them birth. What emerges is a form of "social mind" that solves complex organization problems without conscious cognition. This "social mind" is born of the interaction among all individuals through the rules of institutions that have to date survived cultural selection processes.[90]

While no approach will guarantee perfect cybersecurity outcomes, the informal and formal governance mechanisms mentioned above constitute a polycentric order in which solutions compete to improve baseline cybersecurity.

V. Role of Risk, Uncertainty, and Learning

The only certainty about the future is that it is uncertain. According to Armen Alchian, "uncertainty arises from at least two sources: imperfect foresight and human inability to solve complex problems containing a host of variables even when the optimum is definable."[91] Because risk and uncertainty are features of complex ecosystems such as the Internet of Things, the resilience approach requires its participants to learn from past cyberattacks, embrace contingency, and adapt. Exposure to some risk allows individuals and organizations to evolve and thrive.[92] The capacity for the IoT ecosystem to achieve resilience depends on its ability to learn by experience from exposure to threats. Standing still—the proverbial steady state—increases the system's vulnerability:

> Resilience-thinking does not simply call us into a defensive crouch against uncertainty and risk. Instead, by encouraging adaption, agility, cooperation, connectivity, and diversity, resilience-thinking can bring us to a different way of being in the world, and to a deeper engagement with it. Bolstering our chances of surviving the next shock is important, but it's hardly the sole benefit.[93]

Those who learn by experience are inoculated against disruption caused by similar cyberattacks in the future and improve their ability to improvise and respond.

Managing risk in the IoT ecosystem is difficult because "safety and danger coexist in the same objects and practices."[94] An IP security camera can allow you to spot an intruder, but an insecure IP camera can let an intruder monitor you. Developing resilience relies on organizational learning as well as on systems' ability to repair or transform themselves. It allows for dynamic response—"the ability of a person a firm or an economy to adapt itself to new circumstances by generating new alternatives"—on the part of the stakeholders involved in the process.[95] Importantly, "if the parts of a system are prevented from facing risks, the whole will become unable to adapt to new dangers."[96] By contrast, trial-and-error risk taking, rather than risk aversion, by a variety of key players is the ideal strategy for securing the IoT. As Wildavsky states, "Attempting to short-circuit this competitive, evolutionary, trial and error process by wishing the end—safety—without providing the means—decentralized search—is bound to be self-defeating."[97] Trying out solutions on a small scale enables stakeholders to better sample unknown risks.

Achieving resilience doesn't mean achieving complete cybersecurity; it means making security a habit. Building this habit, or "adaptive capacity," means wrestling with a certain degree of insecurity. According to Nassim Nicholas Taleb, exposure to risk, uncertainty, disorder, volatility, and randomness can lead to

90 Smith, 324.
91 Armen A. Alchian, "Uncertainty, Evolution, and Economic Theory," *Journal of Political Economy* 58, no. 3 (1950): 211–21.
92 Adam D. Thierer, "Failing Better: What We Learn by Confronting Risk and Uncertainty," in *Nudge Theory in Action: Behavioral Design in Policy and Markets*, ed. Sherzod Abdukadirov, Palgrave Advances in Behavioral Economics (n.p.: Palgrave Macmillan, 2016).
93 Zolli and Healy, *Resilience*, 16.
94 Wildavsky 1988, 5.
95 Wildavsky, 6.
96 Wildavsky, 6.
97 Wildavsky, 246.

"antifragility," or systems that improve after experiencing stressors.[98] Maersk's experience with a catastrophic cyberattack demonstrates the importance of giving companies the space to adapt to emerging threats. In June 2017, a group of Russian military hackers released a piece of malware (since dubbed NotPetya) that corrupted machines as far apart as Pennsylvania and Tasmania and crippled Maersk, the world's largest shipping container company. Data from Maersk's terminals around the world were wiped, meaning ships could not unload and new orders could not be taken. As a result, hundreds of trucks backed up at shipyards and ships stalled in the open ocean.

Building resilience into public and private operations is critical to the survival of organizations, allowing them to weather attacks and ensure that the same attack will not cripple them twice. In the wake of NotPetya, Maersk's leaders set up a recovery center at its IT headquarters in Maidenhead, England; flew in regional experts; housed them in every available hotel; purchased new hardware; and hired the consultancy firm Deloitte to rebuild its global network. The company leveraged outside expertise and local knowledge from its own staff to fix the situation and get the company up and running again. Managers were given free rein to use their specific knowledge to do what needed to be done to get their own sectors operational. They were able to locate the single remaining copy of their shipping database on a computer in Ghana. A Ghanaian employee escorted the database to Nigeria for a handoff, to get around visa restrictions preventing Maersk's Ghana-based staff from traveling directly to London. Management learned from the experience and instituted new processes, including redundant system backups that prioritized cybersecurity improvements.[99]

Maersk's recovery demonstrates how empowering entrepreneurs on the ground, introducing redundancy in the form of backups, and instituting processes for learning from cyberattacks are critical features of building resilience to future cyberattacks. James Scott explains, "Complex, diverse, animated environments contribute to producing a resilient, flexible, adept population that has more experience in confronting novel challenges and taking initiative."[100] By contrast, ignoring the radical contingency of the future and suppressing individuals' ability to respond artfully to transient, turbulent, ambiguous situations all but guarantees systemic failure.[101] Regulatory compliance can limit the flexibility of companies to respond to issues as they arise. In the case of the GDPR, the prospect of compliance was enough to prompt thousands of American firms to either shut down or stop serving EU customers.[102] Notably, the Payment Card Industry Security Standards (commonly known as the PCI standard) faces accusations that it is burdensome, overly complex, and "behind the curve": "Some consider the PCI standard a form of check box security that diverts IT staff from current threats as they struggle with compliance to avoid legal liability."[103] By contrast, guidance that emphasizes performance standards over design standards can place the initiative and burden of proof on the manufacturer, promoting operational flexibility.[104] By contrast, a more formal ordering of cybersecurity rules or mandatory commercial IoT design requirements could foster a false sense of security and compromise adaptive capacity.

For every company like Maersk that weathers the cyber storm, there are companies that go underwater. Companies that resist turbulence rather than embracing it as a feature of a developing IoT ecosystem risk bankruptcy. According to the National Cyber Security Alliance, 60 percent of small and midsized businesses that are hacked go out of business within six months.[105] For example, the subscription software

98 Nassim Nicholas Taleb, *Antifragile: Things That Gain from Disorder* (New York: Random House, 2012).
99 Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
100 Scott, *Seeing Like a State*, 349.
101 Scott, 349.
102 Roslyn Layton, "When Evaluating California Data Regulation, Don't Forget the Thousands of US Firms No Longer Operating in the EU," *AEIdeas* (American Enterprise Institute), 2019.
103 Salane and Misshula 2012, 10.
104 Wildavsky 1988, 156.
105 Ken Barnhart et al., "Cyberthreats and Solutions for Small and Midsize Businesses," Vistage Worldwide Inc., 2018.

company Code Spaces and the promotional company Colorado Timberline underwent such thorough ransomware attacks that financial and reputational damage led to bankruptcy.[106]

One can also contrast Maersk's experience with that of a company that did not change its security posture and did not engage in learning or adaption. This could be for a variety of reasons, such as path dependency, overreliance on cyber insurance, or indecision. BlackBerry's chief technology officer has stated that multinational companies are still not prepared for an attack similar to the one on Maersk, even a year after NotPetya.[107] Following the NotPetya attack, 68 percent of security professionals felt that their enterprise did not make necessary improvements to prevent similar multivector attacks.[108]

The resilience approach is consistent with a certain cultural and institutional environment, one that is permissive to change, experimentation, and entrepreneurship. As political economist Joseph Schumpeter argued, risk, failure and "creative destruction" must be tolerated to achieve long-term betterment.[109] Without risk, there is no progress. The governance system that produces the most entrepreneurship and innovation is the one that promotes decentralized, open-ended trial and error and creates a culture of dynamism.

US policy makers have the opportunity to specify resilience as an overt policy goal. The National Telecommunications and Information Administration's green paper on fostering the advancement of the IoT takes the right approach by encouraging "all parties to work within voluntary consensus standards development bodies to ensure the development, deployment, and interoperability of the IoT environment" and by specifying the role of the US Department of Commerce as one of many players in policy decision-making: "The Department will continue to support IoT standards development that is bottom up and private-sector led."[110] By using their convening power to bring together key players at federal and local levels, policy makers can facilitate a conversation about the role of redundancy, learning, and entrepreneurship in the face of cyberattacks.

VI. Conclusion

The Internet of Things is a complex, global network. The governance challenge facing the IoT ecosystem is unique because of its complexity, its dynamism, and its decentralized and distributed nature. The complexity of the digital ecosystem means that a uniform, strict regulatory approach will discourage innovation and adaptability and offset the ecosystem's capability to manage risk.

The resilience approach is messy and imperfect. Yet it works because it allows stakeholders to pursue a variety of solutions that bring the ecosystem to a manageable level of cyber insecurity. As Wildavsky puts it, "Unless safety is continuously reaccomplished, it will decline."[111]

It cannot be underscored enough that there's no single top-down solution to address cyber insecurity:

> There are no finish lines here and no silver bullets. Resilience is always, perhaps maddeningly, provisional, and its insistence toward holism, longer-term thinking, and less-than-peak efficiency represent real political challenges. Many efforts to achieve it will fail, and even a wildly successful effort to boost it will fade, as now forces of change are brought to bear on a system. Resilience must continuously be refreshed and recommitted to.[112]

106 Pro OnCall Technologies, "3 Companies That Went Out of Business Due to a Security Breach," *InSecurity*, November 6, 2014.
107 John Leyden, "A Year after Devastating NotPetya Outbreak, What Have We Learnt?," *The Register*, June 27, 2018, https://www.theregister.co.uk/2018/06/27/notpetya_anniversary/.
108 Ray Lapena, "Enterprise Security Lacking after WannaCry/NotPetya Attacks," *Tripwire*, August 10, 2017.
109 Joseph Schumpeter, *Capitalism, Socialism, and Democracy* (New York: Harper & Brothers, 1942).
110 National Telecommunications and Information Administration, "Fostering the Advancement of the Internet of Things," Department of Commerce Internet Policy Task Force and Digital Economy Leadership Team, 2017, p. 47.
111 Wildavsky 1988, 225.
112 Zolli and Healy, *Resilience*, 276.

Policy makers should commit to create a policy environment that aims at resilience. The best way to weather large-scale disturbances is to empower a network of polycentric stakeholders at multiple levels to remain persistent in the face of emerging threats. In the case of the IoT, government should not be the sole provider of governance. Industry, governments, consumers, and civil-society stakeholders will have to continue to work together on a variety of efforts to mitigate cyber risk and align incentives to improve the ecosystem as a whole. Institutional experimentation is critical. Alternate methods of governance such as peer production, soft law, and emergent multiorganization networks need to be iterated upon. The right policy environment will allow a range of efforts to evolve, improving overall cybersecurity outcomes in the Internet of Things.