8

Governing the Internet of Everything

Scott J. Shackelford[1]

Since the term was first coined in the late 1990s during a presentation about the benefit of radio-frequency identification (RFID) tags in the retail sector, the "Internet of Things" (IoT) has promised a smart, interconnected global digital ecosystem enabling your toaster to text you when your breakfast is ready, and your sweatshirt to give you status updates during your workout. This rise of "smart products" such as internet-enabled refrigerators and self-driving cars holds the promise to revolutionize business and society. But the smart wave will not stop with stuff owing to related trends such as the "Internet of Bodies" now coming into vogue (Atlantic Council, 2017). It seems that, if anything, humanity is headed toward an "Internet of Everything," which is a term that Cisco helped to pioneer (Evans, 2012).

The Internet of Everything (IoE) takes the notion of IoT a step further by including not only the physical infrastructure of smart devices but also its impacts on people, business, and society. Thus, the IoE may be understood as "the intelligent connection of people, process, data and things[,]" whereas IoT is limited to "the network of physical objects accessed through the Internet" (Banafa, 2016). This broader lens is vital for considering the myriad security and privacy implications of smart devices becoming replete throughout society, and our lives. Other ways to conceptualize the problem abound, such as Bruce Schneier's notion of Internet+, or Eric Schmidt's contention that "the Internet will disappear" given the proliferation of smart devices (Giles, 2018). Regardless, the salient point is that our world is getting more connected, if not smarter, but to date governance regimes have struggled to keep pace with this dynamic rate of innovation.

I thank my wonderful colleagues at the Ostrom Workshop for their suggestions and leadership on the many important topics covered herein, particularly Dan Cole and Mike McGinnis.

[1] Chair, Indiana University-Bloomington Cybersecurity Program; Director, Ostrom Workshop Program on Cybersecurity and Internet Governance; Associate Professor, Indiana University Kelley School of Business. An earlier version of this chapter appeared as Scott J. Shackelford, *Governing the Internet of Everything*, Cardozo Arts & Entertainment Law Journal (2019).

https://doi.org/10.1017/9781108749978.009 Published online by Cambridge University Press

Yet it is an open question whether security and privacy protections can or will scale within this dynamic and complex global digital ecosystem, and whether law and policy can keep up with these developments. As Schneier has argued:

> The point is that innovation in the Internet+ world can kill you. We chill innovation in things like drug development, aircraft design, and nuclear power plants because the cost of getting it wrong is too great. We're past the point where we need to discuss regulation versus no-regulation for connected things; we have to discuss smart regulation versus stupid regulation. (Giles, 2018)

The natural question, then, is whether our approach to governing the IoE is, well, smart? This chapter explores what lessons the Institutional Analysis and Development (IAD) and Governing Knowledge Commons (GKC) frameworks hold for promoting security, and privacy, in an IoE, with special treatment regarding the promise and peril of blockchain technology to build trust in such a massively distributed network. Particular attention is paid to governance gaps in this evolving ecosystem, and what state, federal, and international policies are needed to better address security and privacy failings.

The chapter is structured as follows. It begins by offering an introduction to the IoE for the uninitiated, and continues by applying the IAD and GKC frameworks, emphasizing their application for the IoE. The utility of blockchain technology is next explored to help build trust in distributed systems before summarizing implications for managers and policymakers focusing on the intersection between polycentric governance and cyber peace.

8.1 WELCOME TO THE INTERNET OF EVERYTHING

As ever more stuff – not just computers and smartphones, but thermostats and baby monitors, wristwatches, lightbulbs, doorbells, and even devices implanted in our own bodies – are interconnected, the looming cyber threat can easily get lost in the excitement of lower costs and smarter tech. Indeed, smart devices, purchased for their convenience, are increasingly being used by domestic abusers as a means to harass, monitor, and control their victims (Bowles, 2018). Yet, for all the press that the IoT has received, it remains a topic little understood or appreciated by the public. One 2014 survey, for example, found that fully 87% of respondents had never even heard of the "Internet of Things" (Merriman, 2014). Yet managing the growth of the IoE impacts a diverse set of interests: US national and international security; the competitiveness of firms; global sustainable development; trust in democratic processes; and safeguarding civil rights and liberties in the Information Age.

The potential of IoT tech has arguably only been realized since 2010, and is arguably the result of the confluence of at least three factors: (1) the widespread availability of always-on high-speed Internet connectivity in many parts of the world; (2) faster computational capabilities permitting the real-time analysis of Big Data;

https://doi.org/10.1017/9781108749978.009 Published online by Cambridge University Press

and (3) economies of scale lowering the cost of sensors and chips to manufacturers (Shackelford, 2017). However, the rapid rollout of IoT technologies has not been accompanied by any mitigation of the array of technical vulnerabilities across these devices, highlighting a range of governance gaps that may be filled in reference to the Ostrom Design Principles along with the IAD and GKC frameworks.

8.2 APPLYING THE IAD AND GKC FRAMEWORKS TO THE INTERNET OF EVERYTHING

The animating rationale behind the IAD framework was, quite simply, a lack of shared vocabulary to discuss common governance challenges across a wide range of resource domains and issue areas (Cole, 2014). "Scholars adopting … [the IAD] framework essentially commit to 'a common set of linguistic elements that can be used to analyze a wide diversity of problems,'" including, potentially, cybersecurity and Internet governance. Without such a framework, according to Professor Dan Cole, confusion is common, such as in defining "resource systems" that can include "information, data, or knowledge" in the intellectual property context, with natural resources (Cole, 2014, 51). In the Internet governance context, similar confusion surrounds core terms such as "cyberspace," "information security," and "cybersecurity (Shackelford, 2014). There are also other more specialized issues to consider, such as defining what constitutes "critical infrastructure," and what if any "due diligence" obligations operators have to protect it from cyber attackers. Similarly, the data underlying these systems is subject to a range of sometimes vying legal protections. As Professor Cole argues, "[t]rade names, trade secrets, fiduciary and other privileged communications, evidence submitted under oath, computer code, and many other types of information and flows are all dealt with in various ways in the legal system" (Cole, 2014, 52).

Although created for a different context, the IAD framework can nevertheless improve our understanding of data governance, identify and better understand problems in various institutional arrangements, and aid in prediction under various alternative institutional scenarios (Cole, 2014). Indeed, Professor Ostrom believed that the IAD framework had wide application, which has been born out given that it is among the most popular institutional frameworks used in a variety of studies, particularly those focused on natural commons. The IAD framework is unpacked in Figure 8.1, and its application to IoE governance is analyzed in turn, after which some areas of convergence and divergence with the GKC framework are highlighted.

It can be difficult to exclude users from networks, especially those with valuable trade secrets, given the extent to which they present enticing targets for both external actors and insider threats. With these distinctions in mind, Professor Brett Frischmann, Michael Madison, and Katherine Strandburg have suggested a revised IAD framework for the knowledge commons reproduced in Figure 8.2.

https://doi.org/10.1017/9781108749978.009 Published online by Cambridge University Press

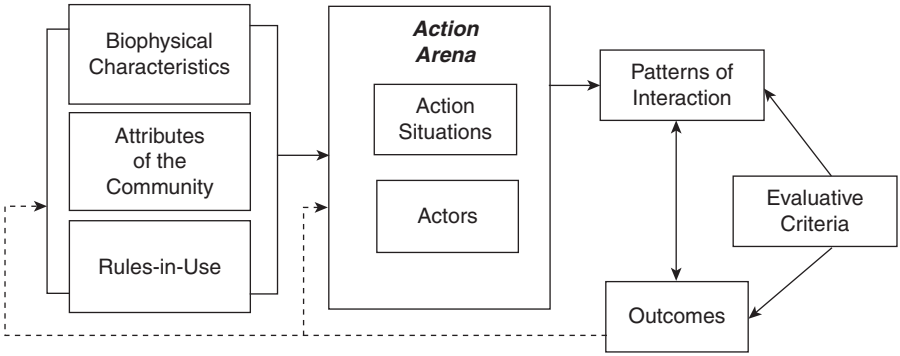

FIGURE 8.1 The Institutional Analysis and Development (IAD) framework

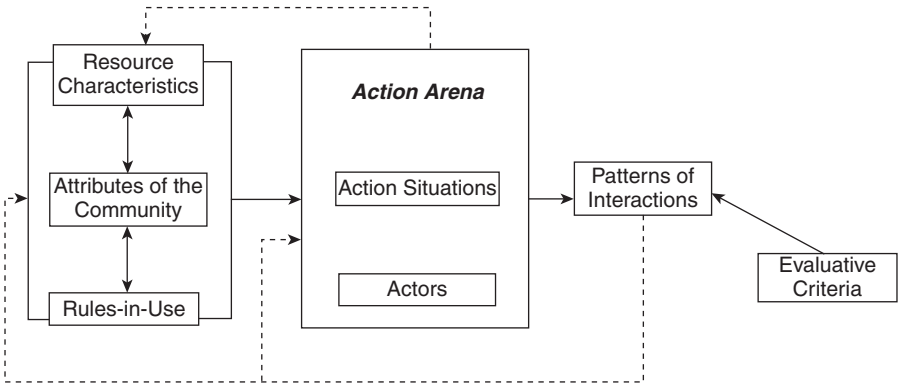

FIGURE 8.2 The Governing Knowledge Commons (GKC) framework

Space constraints prohibit an in-depth analysis of the myriad ways in which the GKC framework might be useful in conceptualizing an array of security and privacy challenges in the IoE, but nevertheless a brief survey is attempted later. In brief, the distinctions with this approach, as compared with the traditional IAD framework, include (1) greater interactions on the left side of the chart underscoring the complex interrelationships in play; (2) the fact that the action area can similarly influence the resource characteristics and community attributes; and (3) that the interaction of rules and outcomes in knowledge commons are often inseparable (Frischmann, Madison and Strandburg, 2014, 19). These insights also resonate in the IoE context, given the tremendous amount of interactions between stakeholders, including IoT device manufacturers, standards-setting bodies, regulators (both national and international), and consumers. Similarly, these interactions are dynamic, given that security compromises in one part of the IoE ecosystem can lay out in a very different

https://doi.org/10.1017/9781108749978.009 Published online by Cambridge University Press

context, as seen in the Mirai botnet, in which compromised smart light bulbs and other IoE devices were networked to crash critical Internet services (Botezatu, 2016).

The following subsections dive into various elements of the GKC framework in order to better understand its utility in conceptualizing IoE governance challenges.

8.2.1 *Resource Characteristics and Classifying Goods in Cyberspace*

Digging into the GKC framework, beginning on the left side of Figure 8.2, there are an array of characteristics to consider, including "facilities through which information is accessed" such as the Internet itself, as well as "artifacts ... including ... computer files" and the "ideas themselves" (Cole, 2014, 10). The "artifacts" category is especially relevant in cybersecurity discussions, given that it includes trade secrets protections, which are closer to a pure private good than a public good and are also the currency of global cybercrime (Shackelford et al., 2015). Internet governance institutions (or "facilities" in this vernacular) can also control the rate at which ideas are diffused, such as through censorship taking subtle (e.g., YouTube's decision to take down Nazi-themed hate speech videos) or extreme (e.g., China's Great Firewall) forms (Beech, 2016).

There is also a related issue to consider: what type of "good" is at issue in the cybersecurity context? In general, goods are placed into four categories, depending on whether they fall on the spectra of exclusion and subtractability (Buck, 1998). Exclusion refers to the relative ease with which goods may be protected. Subtractability evokes the extent to which one's use of a good decreases another's enjoyment of it. If it is easy to exclude others from the use of a good, coupled with a high degree of subtractability, then the type of good is likely to be characterized as "private goods" that are defined by property law and best regulated by the market (Hiller and Shackelford, 2018). Examples in the IoT context are plentiful, from smart speakers to refrigerators. Legal rights, including property rights, to these goods include the right of exclusion discussed above. At the opposite end of the spectrum, where exclusion is difficult and subtractability is low, goods are more likely characterized as "public goods" that might be best managed by governments (Ostrom and Ostrom, 2015). An example is national defense, including, some argue, cybersecurity (Ostrom, 2009). This is an area of some debate, though, given the extensive private sector ownership of critical infrastructure, which makes drawing a clear line between matters of corporate governance and national security difficult.

In its totality, the IoE includes all forms of goods, including private devices and municipal broadband networks, catalyzing a range of positive and negative externalities from network effects to cyberattacks. For example, the IoE includes digital communities as a form of club good, with societies being able to set their own rights of access; a contemporary example is the efforts of Reddit moderators to stop trolls, limit hate speech, and promote a more civil dialogue among users (Roose, 2017). Such communal property rights may either be recognized by the state, or be based

https://doi.org/10.1017/9781108749978.009 Published online by Cambridge University Press

on a form of "benign neglect" (Buck, 1998, 5). Indeed, as of this writing, there is an active debate underway in the United States and Europe about the regulation of social-media platforms to limit the spread of terrorist propaganda, junk news, sex trafficking, and hate speech. Such mixed types of goods are more the norm than the exception. As Cole has argued:

> [S]ince the industrial revolution it has become clear that the atmosphere, like waters, forests, and other natural resources, is at best an impure, subtractable, or congestible public good. As such, these resources fall somewhere on the spectrum between public goods, as technically defined, and club or toll goods. It is such impure public goods to which Ostrom assigned the label "common-pool resources". (Cole, 2014, 54)

Naturally, the next question is whether, in fact, cyberspace may be comparable to the atmosphere as an *impure* public good, since *pure* public goods do not present the same sort of governance challenges, such as the well-studied "tragedy of the commons" scenario, which predicts the gradual overexploitation of common pool resources (Feeny et al., 1990). Though cyberspace is unique given that it can, in fact, expand such as through the addition of new networks (Jordan, 1990), increased use also multiplies threat vectors (Deibert, 2012).

Solutions to the tragedy of the commons typically "involve the replacement of open access with restricted access and use via private property, common property, or public property/regulatory regimes" (Frischmann, Madison, and Strandburg, 2014, 54). However, in practice, as Elinor Ostrom and numerous others have shown, self-organization is in fact possible in practice, as is discussed later (Frischmann, 2018). The growth of the IoE could hasten such tragedies if vulnerabilities replete in this ecosystem are allowed to go unaddressed.

8.2.2 *Community Attributes*

The next box element on the left side of the GKC framework, titled "Attributes of the Community," refers to the network of users making use of the given resource (Smith, 2017). In the natural commons context, communities can be macro (at the global scale when considering the impacts of global climate change) or micro, such as with shared access to a forest or lake. Similarly, in the cyber context, communities come in every conceivable scale and format from private pages on Facebook to peer-to-peer communities to the global community of more than four billion global Internet users as of October 2018, not to mention the billions of devices comprising the IoE. Even such a broad conceptualization omits impacted non-user stakeholders and infrastructure, as may be seen in the push to utilize 5G connectivity, AI, and analytics to power a "safe city" revolution, albeit one built on Huawei architecture. The scale of the multifaceted cyber threat facing the public and private sector parallels in complexity the battle to combat the worst effects of global climate

https://doi.org/10.1017/9781108749978.009 Published online by Cambridge University Press

change (Cole, 2014; Shackelford, 2016). Such a vast scale stretches the utility of the GKC framework, which is why most efforts have considered subparts, or clubs, within this digital ecosystem.

An array of polycentric theorists, including Professor Ostrom, have extolled the benefits of small, self-organized communities in the context of managing common pool resources (Ostrom, 1999). Anthropological evidence has confirmed the benefits of small-scale governance. However, micro-communities can ignore other interests, as well as the wider impact of their actions, online and offline (Murray, 2007). A polycentric model favoring bottom-up governance but with a role for common standards and baseline rules so as to protect against free riders may be the best-case scenario for IoE governance, as is explored further. Such self-regulation has greater flexibility to adapt to dynamic technologies faster than top-down regulations, which even if enacted, can result in unintended consequences, as seen now in the debates surrounding California's 2018 IoT law. As of January 2020, this law would require "any manufacturer of a device that connects 'directly or indirectly' to the Internet . . . [to] equip it with 'reasonable' security features, designed to prevent unauthorized access, modification, or information disclosure" (Robertson, 2018). Yet, it is not a panacea, as we will see, and there is plentiful evidence that simple rule sets – especially when they are generated in consultation with engaged and empowered communities – can produce better governance outcomes.

8.2.3 *Rules-in-Use*

This component of the GKC framework comprises both community norms along with formal legal rules. One of the driving questions in this area is identifying the appropriate governance level at which to formalize norms into rules, for example, whether that is at a constitutional level, collective-choice level, etc. (Cole, 2014, 56). That is easier said than done in the cybersecurity context, given the wide range of industry norms, standards – such as the National Institute for Standards and Technology Cybersecurity Framework (NIST CSF) – state-level laws, sector-specific federal laws, and international laws regulating everything from banking transactions to prosecuting cybercriminals. Efforts have been made to begin to get a more comprehensive understanding of the various norms and laws in place, such as through the International Telecommunication Union's (ITU)'s Global Cybersecurity Index and the Carnegie Endowment International Cybersecurity Norms Project, but such efforts remain at an early stage of development. A variety of rules may be considered to help address governance gaps, such as position and choice rules that define the rights and responsibilities of actors, such as IoT manufacturers and Internet Service Providers (ISPs), as is shown in Table 8.1 (Ostrom and Crawford, 2005). Given the degree to which core critical infrastructure – such as smart grids and Internet-connected medical devices – are also subsumed within IoT debates, there is a great deal of overlap between potential rule sets from incentivizing

https://doi.org/10.1017/9781108749978.009 Published online by Cambridge University Press

TABLE 8.1 *Types of rules*

Aggregation rules	Determine whether a decision by a single actor or multiple actors is needed prior to acting at a decision point in a process.
Boundary rules	Define: 1. who is eligible to take a position; 2. the process for choosing who is eligible to take a position; 3. how actors can leave positions; 4. whether anyone can hold multiple positions simultaneously; and 5. succession to vacant positions.
Choice rules	Define what actors in positions must, must not, or may do in their position and in particular circumstances.
Information rules	Specify channels of communication among actors, as well as the kinds of information that can be transmitted between positions.
Payoff rules	Assign external rewards or sanctions for particular actions or outcomes.
Position rules	Define positions that actors hold, including as owners of property rights and duties.

the use of cybersecurity standards and frameworks, as is happening in Ohio to hardening supply chains.

Many of these rules have cyber analogues, which emphasize cybersecurity information sharing through public–private partnerships to address common cyber threats, penalize firms and even nations for lax cybersecurity due diligence, and define the duties – including liability – of actors, such as Facebook and Google (Reardon, 2018).

The question of what governance level is most appropriate to set the rules for IoT devices is pressing, with an array of jurisdictions, including California, pressing ahead. For example, aside from its IoT-specific efforts, California's 2018 Consumer Privacy Act is helping to set a new transparency-based standard for US privacy protections. Although not comparable to the EU's new General Data Protection Regulation (GDPR) discussed later, it does include provisions that allow consumers to sue over data breaches, including in the IoT context, and decide when, and how, their data is being gathered and used by companies (Adler, 2018). Whether such state-level action, even in a state with an economic footprint as the size of California, will help foster enhanced cybersecurity due diligence across the broader IoE ecosystem remains to be seen.

8.2.4 *Action Arenas*

The arena is just that, the place where decisions are made, where "collective action succeeds or fails" (Cole, 2014, 59). Such arenas exist at three levels within the GKC framework – constitutional, collective-choice, and operational. Decisions made at each of these governance levels, in turn, impact a range of rules and community

https://doi.org/10.1017/9781108749978.009 Published online by Cambridge University Press

attributes, which is an important feature of the framework. Examples of decision-makers in each arena in the cybersecurity context include (1) at the constitutional level, judges deciding the bounds of "reasonable care" and "due diligence" (Shackleford, 2015); (2) federal and state policymakers at the collective-choice (e.g., policy) level, such as the Federal Trade Commission (FTC) policing unfair and deceptive trade practices; and (3) at the operational level, firms, households, and everyone else.

8.2.5 *Evaluation Criteria*

The final component, according to Cole, is "the most neglected and underdeveloped" of the frameworks (Cole, 2014, 62). Elinor Ostrom, for example, offered the following "evaluative criteria" in considering how best to populate it, including "(1) economic efficiency; (2) fiscal equivalence; (3) redistributional equity; (4) accountability; (5) conformance to values of local actors; and (6) sustainability" (Cole, 2014, 62). In the GKC context, these criteria might include "(1) increasing scientific knowledge; (2) sustainability and preservation; (3) participation standards; (4) economic efficiency; (5) equity through fiscal equivalence; and (6) redistributional equity" (Hess and Ostrom, 2007, 62). This lack of rigor might simply be due to the fact that, in the natural commons context, the overriding goal has been "long-run resource sustainability" (Cole, 2014, 62). It is related, in some ways, to the "Outcomes" element missing from the GKC framework but present in the IAD framework, which references predictable outcomes of interactions from social situations, which can include consequences for both resource systems and units. Although such considerations are beyond the findings of the IAD framework, in the cybersecurity context, an end goal to consider is defining and implementing cyber peace.

"Cyber peace," which has also been called "digital peace," is a term that is increasingly used, but it also remains an arena of little consensus. It is clearly more than the "absence of violence" online, which was the starting point for how Professor Johan Galtung described the new field of peace studies he helped create in 1969 (Galtung, 1969). Similarly, Galtung argued that finding universal definitions for "peace" or "violence" was unrealistic, but rather the goal should be landing on an apt "subjectivistic" definition agreed to by the majority (Galtung, 1969, 168). He undertook this effort in a broad, yet dynamic, way recognizing that as society and technology changes, so too should our conceptions of peace and violence. That is why he defined violence as "the cause of the difference between the potential and the actual, between what could have been and what is" (Galtung, 1969, 168).

Cyber peace is defined here not as the absence of conflict, what may be called negative cyber peace. Rather, it is the construction of a network of multilevel regimes that promote global, just, and sustainable cybersecurity by clarifying the rules of the road for companies and countries alike to help reduce the threats of

cyber conflict, crime, and espionage to levels comparable to other business and national security risks. To achieve this goal, a new approach to cybersecurity is needed that seeks out best practices from the public and private sectors to build robust, secure systems, and couches cybersecurity within the larger debate on Internet governance. Working together through polycentric partnerships of the kind described later, we can mitigate the risk of cyber war by laying the groundwork for a positive cyber peace that respects human rights, spreads Internet access along with best practices, and strengthens governance mechanisms by fostering multi-stakeholder collaboration (Galtung, 2012). The question of how best to achieve this end is open to interpretation. As Cole argues, "[f]rom a social welfare perspective, some combination of open- and closed-access is overwhelmingly likely to be more socially efficient than complete open or close-access" (Cole, 2014, 61). Such a polycentric approach is also a necessity in the cyber regime complex, given the prevalence of private and public sector stakeholder controls.

In the cybersecurity context, increasing attention has been paid identifying lessons from the green movement to consider the best-case scenario for a sustainable cyber peace. Indeed, cybersecurity is increasingly integral to discussions of sustainable development – including Internet access – which could inform the evaluative criteria of a sustainable cyber peace in the IoE. Such an approach also accords with the "environmental metaphor for information law and policy" that has been helpful in other efforts (Frischmann, Madison, and Strandburg, 2014, 16).

It is important to recognize the polycentric nature of the IoE to ascertain the huge number of stakeholders – including users – that can and should have a say in contributing to legitimate governance. Indeed, such concerns over "legitimate" Internet governance have been present for decades, especially since the creation of the Internet Corporation for Assigned Names and Numbers (ICANN). Given the pushback against that organization as a relatively top-down artificial construct as compared to the more bottom-up Internet Engineering Task Force (IETF), legitimacy in the IoE should be predicated to the extent possible locally through independent (and potentially air gapped) networks, Internet Service Providers (ISPs), and nested state, federal, and international law. To conceptualize such system, the literature on regime complexes might prove helpful, which is discussed next in the context of blockchain technology.

8.3 IS BLOCKCHAIN THE ANSWER TO THE IOE'S WOES?

Professor Ostrom argued that "[t]rust is the most important resource" (Escotet, 2010). Indeed, the end goal of any governance institution is arguably trust – how to build trust across users to attain a common goal, be it sustainable fishery management or securing the IoE. The GKC framework provides useful insights toward this end. But one technology could also help in this effort, namely blockchain, which, according to Goldman Sachs, could "change 'everything'" (Lachance, 2016). Regardless of the

https://doi.org/10.1017/9781108749978.009 Published online by Cambridge University Press

question being asked, some argue that it is the answer to the uninitiated – namely, a blockchain cryptographic distributed ledger (Trust Machine, 2015). Its applications are widespread, from recording property deeds to securing medical devices. As such, its potential is being investigated by a huge range of organizations, including US Defense Advanced Research Projects Agency (DARPA), IBM, Maersk, Disney, and Greece, the latter of which is seeking to leverage blockchain to help enhance social capital by helping to build trust around common governance challenges, such as land titling (Casey and Vigna, 2018). Examples similarly abound regarding how firms use blockchains to enhance cybersecurity. The technology could enable the Internet to become decentralized, pushing back against the type of closed platforms analyzed by Professor Johnathan Zittrain and others (Zittrain, 2008). Already, a number of IoT developers are experimenting with the technology in their devices; indeed, according to one recent survey, blockchain adoption in the IoT industry doubled over the course of 2018 (Zmudzinski, 2019).

Yet formidable hurdles remain before blockchain technology can be effectively leveraged to help promote sustainable development, peace, and security in the IoE. No blockchain, for example, has yet scaled to the extent necessary to search the entire web. There are also concerns over hacking and integrity (such as when a single entity controls more than fifty percent of the processing power), including the fact that innovation is happening so quickly that defenders are put in a difficult position as they try to build resilience into their distributed systems (Villasenor, 2018). But the potential for progress demands further research, including how it could help promote a polycentric cyber peace in the burgeoning IoE.

8.4 POLYCENTRIC IMPLICATIONS

As Professor Cole has maintained, "those looking for *normative* guidance from Ostrom" and the relevant governance frameworks and design principles discussed herein are often left wanting (Cole, 2014, 46). Similar to the big questions in the field of intellectual property, such as defining the optimal duration of a copyright, it stands to reason, then, that the Ostroms' work might tell us relatively little about the goal of defining, and pursuing, cyber peace. An exception to the Ostroms' desire to eschew normative suggestions, though, is polycentric governance, which builds from the notion of subsidiarity in which governance "is a 'co-responsibility' of units at central (or national), regional (subnational), and local levels" (Cole, 2014, 47).

For purposes of this study, the polycentric governance framework may be considered to be a multi-level, multi-purpose, multi-functional, and multi-sectoral model that has been championed by numerous scholars, including the Ostroms (Mcginnis, 2011). It suggests that "a single governmental unit" is usually incapable of managing "global collective action problems" such as cyber-attacks (Ostrom, 2009,

35). Instead, a polycentric approach recognizes that diverse organizations working at multiple scales can enhance "flexibility across issues and adaptability over time" (Keohane and Victor, 2011, 15). Such an approach can help foster the emergence of a norm cascade improving the Security of Things (Finnemore and Sikkink, 1998, 895).

Not all polycentric systems are guaranteed to be successful. Disadvantages, for example, can include gridlock and a lack of defined hierarchy (Keohane and Victor, 2011). Yet progress has been made on norm development, including cybersecurity due diligence, discussed later, which will help IoT manufacturers better fend off attacks against foreign nation states. Still, it is important to note that even the Ostroms' commitment to polycentric governance "was contingent, context-specific, and focused on matching the scale of governance to the scale of operations appropriate for the particular production or provision problem under investigation" (Cole, 2014, 47). During field work in Indianapolis, IN, for example, the Ostroms found that, in fact, medium-sized police departments "outperformed both smaller (neighborhood) and larger (municipal-level) units" (Cole, 2014, 47). In the IoE context, as has been noted, the scale could not be greater with billions of people and devices interacting across myriad sectors, settings, and societies. The sheer complexity of such a system, along with the history of Internet governance to date, signals that there can be no single solution or governance forum to foster cyber peace in the IoE. Rather, polycentric principles gleaned from the GKC framework should be incorporated into novel efforts designed to glean the best governance practices across a range of devices, networks, and sectors. These should include creating clubs and industry councils of the kind that the GDPR is now encouraging to identify and spread cybersecurity best practices, leveraging new technologies such as blockchain to help build trust in this massively distributed system, and encouraging norm entrepreneurs like Microsoft and the State of California to experiment with new public–private partnerships informed by the sustainable development movement. Success will be difficult to ascertain as it cannot simply be the end of cyber attacks. Evaluation criteria are largely undefined in the GKC framework, as we have seen, which the community should take as a call to action, as is already happening by members of the Cybersecurity Tech Accord and the Trusted IoT Alliance.

Such efforts may be conceptualized further within the literature on the cyber regime complex. As interests, power, technology, and information diffuse and evolve over time within the IoE, comprehensive regimes are difficult to form. Once formed, they can be unstable. As a result, "rarely does a full-fledged international regime with a set of rules and practices come into being at one period of time and persist intact" (Keohane and Victor, 2011, 9). According to Professor Oran Young, international regimes emerge as a result of "codifying informal rights and rules that have evolved over time through a process of converging expectations or tacit bargaining" (Young, 1997, 10). Consequently, regime complexes, as a form of bottom-up institution building, are becoming relatively more popular in both the

climate and Internet governance contexts, which may have some benefits since negotiations for multilateral treaties could divert attention from more practical efforts to create flexible, loosely coupled regimes (Keohane and Victor, 2011). An example of such a cyber regime complex may be found in a work by Professor Joseph S. Nye, Jr., which is reproduced in Figure 8.3.

But there are also the costs of regime complexes to consider. In particular, such networks are susceptible to institutional fragmentation and gridlock. And there are moral considerations about such regime complexes. For example, in the context of climate change, these regimes omit nations that are not major emitters, such as the least developed nations that are the most at risk to the effects of a changing climate. Similar arguments could play out in the IoE context with some consumers only being able to access less secure devices due to jurisdictional difference that could impinge on their privacy. Consequently, the benefits of regime complexes must be critically analyzed. By identifying design rules for the architecture, interfaces, and integration protocols within the IoE, both governance scholars and policymakers may be able to develop novel research designs and interventions to help promote cyber peace.

8.5 CONCLUSION

As Cole has argued, "there are no institutional panaceas for resolving complex social dilemmas" (Cole, 2014, 48). Never has this arguably been truer than when considering the emerging global digital ecosystem here called the IoE. Yet, we ignore the history of governance investigations at our peril, as we look ahead to twenty-first century global collective action problems such as promoting cyber peace in the IoE. Important questions remain about the utility of the Ostrom Design Principles, the IAD, and GKC frameworks in helping us govern the IoE. Even more questions persist about the normative goals in such an enterprise, for example, what cyber peace might look like and how we might be able to get there. That should not put off scholars interested in this endeavor. Rather, it should be seen as a call to action. The stakes could not be higher. Achieving a sustainable level of cybersecurity in the IoE demands novel methodologies, standards, and regimes. The Ostroms' legacy helps to shine a light on the path toward cyber peace.

REFERENCES

Adler, Ben. "California Passes Strict Internet Privacy Law with Implications for The Country." *NPR*. June, 2018.

Ashton, Kevin. "That 'Internet of Things' Thing." RFID Journal, June, 2009.

Banafa, Ahmed. "The Internet of Everything (IOE)." *Open Mind*, August, 2016.

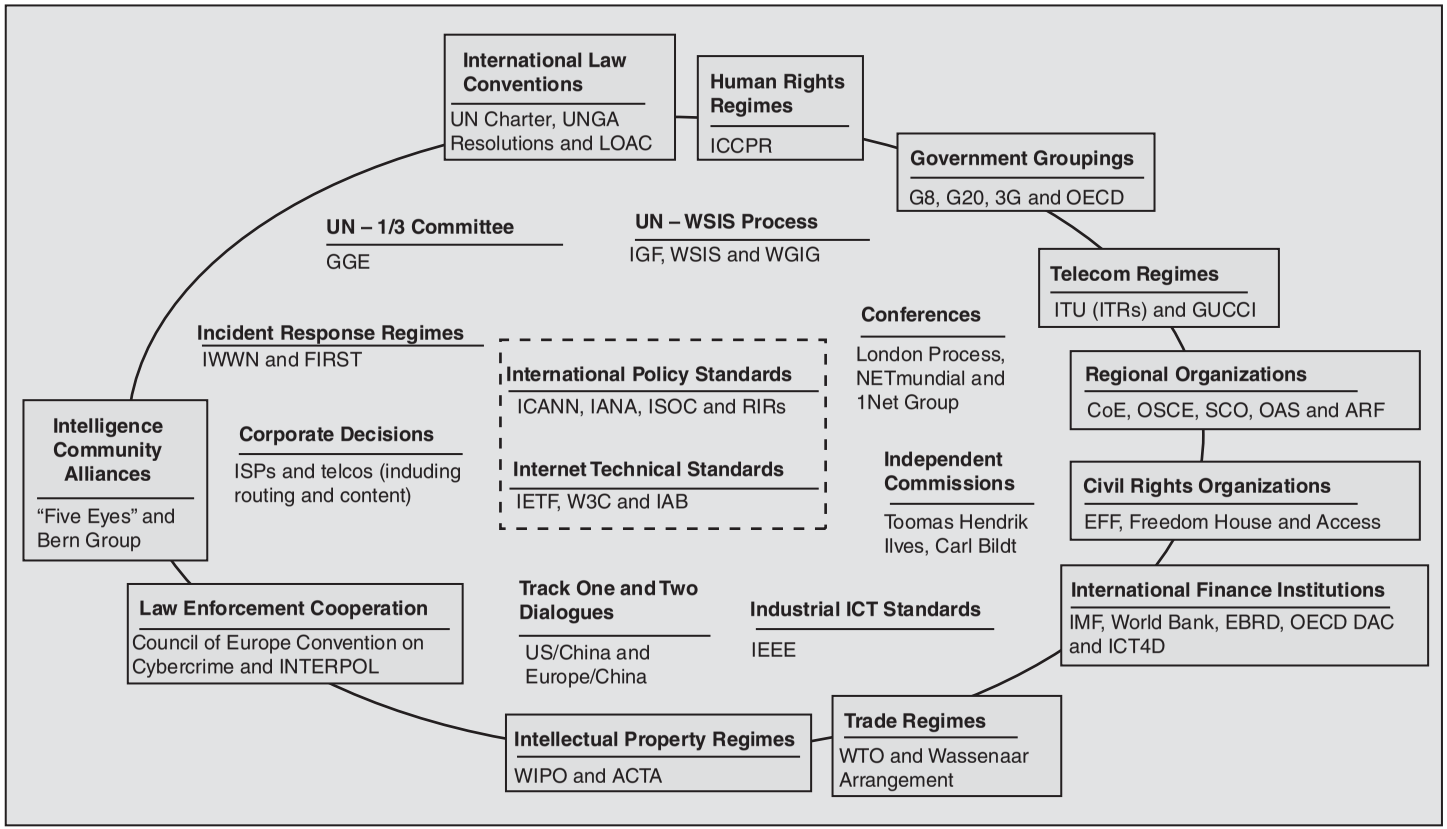

FIGURE 8.3 Cyber regime complex map (Nye, 2014, 8)

Beech, Hannah. "China's Great Firewall is Harming Innovation, Scholars Say." *Time*, June 2016.
Botezatu, Bogdan. "Unprotected IoT Devices Killed the US Internet for Hours." *Bitdefender*, October, 2016.
Bowles, Nellie. "Thermostats, Locks and Lights: Digital Tools of Domestic Abuse." *New York Times*, June, 2018.
Buck, Susan J. *The Global Commons: An Introduction*. New York: Island Press, 1998.
Casey, Michael J. and Vigna, Paul. *The Truth Machine: The Blockchain and the Future of Everything*. New York: St. Martin's Press, 2018.
Cole, Dan. "Learning from Lin: Lessons and Cautions from the Natural Commons for the Knowledge Commons." In *Governing Knowledge Commons*, Edited by Brett M. Frischmann, Michael J. Madison, and Katherine J. Strandburg, 1st ed. Oxford University Press, 2014.
"Cyber Risk Thursday: Internet of Bodies." *Atlantic Council*, September, 2017.
Deibert, Ron. "Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace." Canadian Defense and Foreign Affairs Institute, 2012.
Evans, Dave. "The Internet of Everything: How More Relevant and Valuable Connections Will Change the World." *Cisco*, 2012.
Feeny, David, Berkes, Fikret, Mccay, Bomnnie J., and Acheson, James M. "The Tragedy of the Commons: Twenty-Two Years Later." *Human Ecology*, 18 (March 1990): 1–19.
Finnemore, Martha and Sikkink, Kathryn. "International Norm Dynamics and Political Change." *International Organization*, 52 (1998): 887–917.
Frischmann, Brett. "The Tragedy of the Commons, Revisited." *Scientific American*, November, 2018.
Frischmann, Brett M., Madison, Michael J., and Strandburg, Katherine J., eds. *Governing knowledge commons*. Oxford University Press, 2014.
Galtung, Johan. "Peace, Positive and Negative." *In The Encyclopedia of Peace Psychology*. Edited by Daniel J. Christie. Oxford, UK: Wiley-Blackwell, 2012.
Galtung, Johan. "Violence, Peace, and Peace Research." *Peace Research*, 6, 3 (1969): 167–191.
Giles, Martin. "For Safety's Sake, We Must Slow Innovation in Internet-Connected Things." *MIT Technology Review*. September, 2018.
Hiller, Janine and Shackelford, Scott J. "The Firm and Common Pool Resource Theory: Unpacking the Rise of Benefit Corporations." *American Business Law Journal*, 55, 1 (2018): 5–51.
Interview with Nobel Laureate Elinor Ostrom, Escotet Found., http://escotet.org/2010/11/interview-with-nobel-laureate-elinor-ostrom/ (last visited June 29, 2018).
Keohane, Robert O. and Victor, David G. "The Regime Complex for Climate Change." *Perspectives on Politics*, 9, 1 (2011): 7–23.
Johnson, Gregoray A. "Organizational Structure and Scalar Stress." In *Theory and Explanation in Archeology*, Edited by Colin Renfrew, Michael Rowlands and Barbara A. Segraves-Whallon, Academic Press, Inc., 1982.
Jordan, Tim. *Cyberpower: The Culture and Politics of Cyberspace and the Internet*. London: Routledge Press, 1999.
Lachance, Naomi. "Not Just Bitcoin: Why the Blockchain Is a Seductive Technology to Many Industries." *NPR*, May, 2016.
McGinnis, Michael D. "An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework." Policy Studies, 39, 1 (2011): 169–183.
Merriman, Chris. "87 Percent of Consumers Haven't Heard of the Internet of Things." *Inquirer*, August, 2014.

Murray, Andrew. *The Regulation of Cyberspace: Control in the Online Environment*. London: Routledge, 2007.
Nye, Joseph S. "The Regime Complex for Managing Global Cyber Activities." *Global Commission on Internet Governance*, 2014.
Ostrom, Vincent and Ostrom, Elinor. "Public Goods and Public Choices." In *Elinor Ostrom and the Bloomington School of Political Economy Vol. 2*, Edited by Daniel H. Cole and Michael McGinnis, Lexington Books, 2015.
Ostrom, Elinor. "Beyond Markets and States: Polycentric Governance of Complex Economic Systems." Nobel Prize Lecture, 2009.
Ostrom, Elinor. "A Polycentric Approach for Coping with Climate Change." *World Bank Policy Research*, 35, 5095 (2009).
Ostrom, Elinor and Hess, Charlotte. "A Framework for Analyzing the Knowledge Commons." *In Understanding Knowledge as a Commons: From Theory to Practice*. Edited by Charlotte Hess and Elinor Ostrom, London: MIT Press, 2007.
Ostrom, Elinor and Crawford, Sue. "Classifying Rules." In *Understanding Institutional Diversity*. Edited by Elinor Ostrom. Princeton, NJ: Princeton University Press, 2005.
Ostrom, Elinor, Burger, Joanna, Field, Christopher B., Norgaard, Richard B., and Policansky, David, "Revisiting the Commons: Local Lessons, Global Challenges." *Science*, April, 1999.
Reardon, Marguerite. "Facebook's FTC Consent Decree Deal: What You Need to Know." *CNet*, August, 2018.
Robertson, Adi. "California Just Became the First State with an Internet of Things Cybersecurity Law." *Verge*. September, 2018.
Roose, Kevin. "Reddit Limits Noxious Content by Giving Trolls Fewer Places to Gather." New York Times, September, 2017.
Shackelford, Scott J., Raymond, Anjanette, Charoen, Danuvasin, Balakrishnan, Rakshana, Dixit, Prakhar, Gjonaj, Julianna, and Kavi, Rachith. "When Toasters Attack: Enhancing the 'Security of Things' through Polycentric Governance." *University of Illinois Law Review*, 2017: 415.
Shackelford, Scott J. "On Climate Change and Cyber Attacks: Leveraging Polycentric Governance to Mitigate Global Collective Action Problems." *Vanderbilt Journal of Entertainment and Technology Law*, 18 (2016): 653–711.
Shackelford, Scott J., Richards, Eric L., Raymond, Anjanette H., and Craig, Amanda N., "Using BITs to Protect Bytes: Promoting Cyber Peace and Safeguarding Trade Secrets through Bilateral Investment Treaties." *American Business Law Journal*, 52 (2015): 1–74.
Shackelford, Scott J., Proia, Andrew, Craig, Amanda, and Martell, Brenton. "Toward a Global Standard of Cybersecurity Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices." *Texas International Law Journal*, 50 (2015): 287.
Shackelford, Scott J. *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*. Washington, DC: Cambridge University Press, 2014.
Smith, Michael. "The Tragedy of the Commons' in the IoT Ecosystem." *Computerworld*, August, 2017.
The Promise of the Blockchain: The Trust Machine, *Economist*, October, 2015.
Villasenor, John. "Blockchain Technology: Five Obstacles to Mainstream Adoption." *Forbes*, June, 2018.
Young, Oran R. "Rights, Rules, and Resources in World Affairs." *In Global Governance: Drawing Insights from the Environmental Experience*. Edited by Oran R. Young. New Haven: MIT Press, 1997.

Zittrain, Jonathan. *The Future of the Internet and How to Stop It*. New Haven: Yale University Press, 2008.
Zmudzinski, Adrian. "Blockchain Adoption in IoT Industry More Than Doubled in 2018: Survey." *Cointelegraph*, January, 2019.
Waltl, Josef. *IP Modularity in Software Products and Software Platform Ecosystems*.

https://doi.org/10.1017/9781108749978.009 Published online by Cambridge University Press