GOVERNING THE INTERNET OF EVERYTHING♦

SCOTT J. SHACKELFORD JD, PHD*

ABSTRACT

Since the term was first coined in the late 1990s, the "Internet of Things" has promised a smart, interconnected world 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 appliances has the potential to revolutionize both business and society. But the smart wave will not stop with stuff, with related trends such as the Internet of Bodies now coming into vogue. It seems that, if anything, humanity is headed toward an Internet of Everything. Yet it is an open question whether security and privacy protections can or will scale along with this increasingly crowded field, and whether law and policy can keep up with these developments. This Article explores what lessons the Institutional Analysis and Development (IAD) and Governing Knowledge Commons (GKC) Frameworks hold for promoting security and privacy, in an Internet of Everything, 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.

INTRODUCTION

Since the term was first coined in the late 1990s,[1] the "Internet of Things" has promised a smart, interconnected world enabling your toaster to text you when your breakfast is ready, and your sweatshirt to give you status updates during your workout.[2] This rise of "smart products" holds the promise to revolutionize business and society. But the smart wave will not stop with objects, with related trends such as the Internet of Bodies now coming into vogue.[3] It seems that, if anything, humanity is headed toward an Internet of Everything (IoE), which,

* Chair, Indiana University-Bloomington Cybersecurity Program; Director, Ostrom Workshop Program on Cybersecurity and Internet Governance; Associate Professor, Indiana University Kelley School of Business. A version of this Article will be republished as a book chapter in a forthcoming volume in the Cambridge Studies on Governing Knowledge Commons series tentatively entitled, "Privacy as Knowledge Commons Governance."

[1] Kevin Ashton, *That 'Internet of Things' Thing*, RFID J. (June 22, 2009), https://www.rfidjournal.com/articles/view?4986.

[2] *See, e.g.*, Chris Ziegler, *Finally, There's a Hoodie that Can Text Your Mom*, VERGE (June 8, 2014, 4:57 PM), https://www.theverge.com/mobile/2014/6/8/5791464/finally-theres-a-hoodie-that-can-text-your-mom.

[3] *See Cyber Risk Thursday: Internet of Bodies*, ATLANTIC COUNCIL (Sept. 21, 2017), http://www.atlanticcouncil.org/events/webcasts/cyber-risk-thursday-internet-of-bodies.

according to Cisco, involves "bringing together people, process, data, and things to make networked connections more relevant and valuable than ever before—turning information into actions that create new capabilities, richer experiences, and unprecedented economic opportunity for businesses, individuals, and countries."[4] Other ways to conceptualize the problem abound are Bruce Schneier's notion of Internet+, or Eric Schmidt's contention that "the Internet will disappear" given the proliferation of smart devices.[5] Regardless, the salient point is that our world is becoming more connected, if not smarter, but to date, governance regimes have struggled to keep pace with this dynamic rate of innovation.

It is an open question whether security and privacy protections can or will scale along with this increasingly crowded field. As Schneier has argued,

> [t]he 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.[6]

Martin Giles, in his article, explores what lessons the Institutional Analysis and Development (IAD) and Governing Knowledge Commons (GKC) Frameworks hold for promoting security, and privacy, in an Internet of Everything, including whether they might help inform the creation of such smart regulation for an increasingly smart world. It does not undertake an in-depth regulatory analysis of existing IoT regimes, since this has been done previously,[7] though it does analyze specific instances that are illustrative of findings from this literature, such as the work of the National Institute for Standards and Technology. Rather, the focus here is on assessing findings from the social science research on governance to identify both best practices and investigate policy implications. For the first time, for example, the

---

[4] Ahmed Banafa, *The Internet of Everything*, OPEN MIND (Aug. 29, 2016), https://www.bbvaopenmind.com/en/the-internet-of-everything-ioe/.

[5] *See* Martin Giles, *For Safety's Sake, We Must Slow Innovation in Internet-connected Things*, MIT TECH. REV. (Sept. 6, 2018), https://www.technologyreview.com/s/611948/for-safetys-sake-we-must-slow-innovation-in-internet-connected-things/; Christina Medici Scolaro, *Why Google's Eric Schmidt Says the 'Internet Will Disappear*,' CNBC (Jan. 23, 2015), https://www.cnbc.com/2015/01/23/why-googles-eric-schmidt-says-the-internet-will-disappear.html.

[6] Giles, *supra* note 5.

[7] *See, e.g.*, Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 547 (2017); Laura DeNardis & Mark Raymond, *The Internet of Things as a Global Policy Frontier*, 51 U.C. DAVIS L. REV. 475, 476 (2017); Jane E. Kirtley & Scott Memmel, *Rewriting the "Book of the Machine": Regulatory and Liability Issues for the Internet of Things*, 19 MINN. J.L. SCI. & TECH. 455, 459 (2018).

groundbreaking IAD and GKC Frameworks are applied to the issue of IoT security, which helps to illustrate governance gaps and what to do about them. Further, special coverage is offered with regards to the promise and peril of blockchain technology to build trust in such a massively distributed network.

This Article is structured as follows. Part I offers an introduction to the Internet of Everything for the uninitiated. Part II then introduces and applies the Ostrom Design Principles in the cyber context. Part III analyzes the IAD and GKC Frameworks, emphasizing their application for the Internet of Everything. Part IV explores the utility of blockchain technology to help build trust in distributed systems. Part V then summarizes implications for managers and policymakers focusing on the intersection between polycentric governance and cyber peace.

I. WELCOME TO THE INTERNET OF EVERYTHING

As more things—from doorbells to medical devices—are interconnected, the looming cyber threat can easily get lost in the excitement over cheaper, smarter tech.[8] Indeed, smart devices, purchased for their convenience, are increasingly being used by domestic abusers as a means to harass, monitor, and control their victims.[9] 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 eighty seven percent of respondents had never even heard of the "Internet of Things."[10] Yet managing the growth of the Internet of Everything impacts a diverse set of interests: U.S. 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.[11]

---

[8] *See* Aaron Tilley, *How Hackers Could Use A Nest Thermostat As An Entry Point Into Your Home*, FORBES (Mar. 6, 2015, 6:00 AM), https://www.forbes.com/sites/aarontilley/2015/03/06/nest-thermostat-hack-home-network/#235d0d693986; Carl Franzen, *How to Find a Hack-Proof Baby Monitor*, OFFSPRING (Aug. 4, 2017, 6:30 PM), https://offspring.lifehacker.com/how-to-find-a-hack-proof-baby-monitor-1797534985; Charlie Osborne, *Smartwatch Security Fails to Impress: Top Devices Vulnerable to Cyberattack*, ZDNET (July 22, 2015, 10:25 PM), http://www.zdnet.com/article/smartwatch-security-fails-to-impress-top-devices-vulnerable-to-cyberattack/; John Markoff, *Why Light Bulbs May Be the Next Hacker Target*, N.Y. TIMES (Nov. 3, 2016), https://www.nytimes.com/2016/11/03/technology/why-light-bulbs-may-be-the-next-hacker-target.html?_r=0.

[9] *See* Nellie Bowles, *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse*, N.Y. TIMES (June 23, 2018), https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html.

[10] *See* Chris Merriman, *87 Percent of Consumers Haven't Heard of the Internet of Things*, INQUIRER (Aug. 22, 2014), https://www.theinquirer.net/inquirer/news/2361672/87-percent-of-consumers-havent-heard-of-the-internet-of-things.

[11] For more on these topics, see SCOTT J. SHACKELFORD, GOVERNING NEW FRONTIERS IN THE INFORMATION AGE (forthcoming 2019).

The potential of IoT tech has, arguably, only been realized since 2010,[12] and is possibly 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; and (3) economies of scale lowering the cost of sensors and chips to manufacturers.[13] 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.

II. UNDERSTANDING THE OSTROM DESIGN PRINCIPLES IN THE CYBER CONTEXT

As Professor Dan Cole has stated, governance scholars have long been mining the Ostroms' work on property regimes governing common-pool resources (CPRs) to better understand their application for contemporary challenges, including the "knowledge commons."[14] Rather than a direct application of the Ostrom Design Principles or the IAD Framework, discussed further below, Professors Elinor Ostrom and Charlotte Hess recognized the distinct nature of natural and artificial commons spaces, which require "systematic study of its own resources, actors, [and] institutions . . . ."[15] After all, these are vastly different resource domains holding unique types of goods, thus requiring novel governance mechanisms and frameworks for understanding the dynamics in play.[16] One should not let the terminology used confuse this effort; after all, Professor Ostrom herself reportedly "regretted confusion arising from the phrase 'design principles' and has suggested 'best practices' as an alternative."[17]

Beginning with the Ostrom Design Principles, Professor Ostrom was "focused on constructing empirically informed frameworks, theories, and models that were (1) conceptually clear; (2) thickly descriptive (embracing complexity); (2) diagnostic; (3) analytically rigorous; and (4) integrative of configural interactions among

[12] *See* Jacob Morgan, *A Simple Explanation Of 'The Internet of Things'*, FORBES (May 13, 2014, 12:05 AM), http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/.

[13] *See* Jim Chase, *The Evolution of the Internet of Things*, TEX. INSTRUMENTS (2013), www.ti.com/lit/ml/swrb028/swrb028.pdf; Scott J. Shackelford et al., *When Toasters Attack: A Polycentric Approach to Enhancing the 'Security of Things'*, 2017 U. ILL. L. REV. 415 (2017).

[14] Dan H. Cole, *Learning from Lin: Lessons and Cautions from the Natural Commons for the Knowledge Commons*, *in* GOVERNING KNOWLEDGE COMMONS 45, 45 (Brett M. Frischmann, Michael J. Madison, & Katherine J. Strandburg eds., 2014).

[15] *Id.*

[16] *Id.* at 46.

[17] *Id.* at 50 n.9.

explanatory factors, suggesting patterns of social interactions and their social-ecological consequences . . . ."[18] This was the thinking behind her groundbreaking work *Governing the Commons*, in which Professor Ostrom created an informative framework of eight design principles for the management of common pool resources.[19] These principles include the importance of: (1) "clearly defined boundaries for the user pool . . . and the resource domain";[20] (2) "proportional equivalence between benefits and costs";[21] (3) "collective choice arrangements" ensuring "that the resource users participate in setting . . . rules";[22] (4) "monitoring . . . by the appropriators or by their agents";[23] (5) "graduated sanctions" for rule violators;[24] (6) "conflict-resolution mechanisms [that] are readily available, low cost, and legitimate";[25] (7) "minimal recognition of rights to organize";[26] and (8) "governance activities [being] . . . organized in multiple layers of nested enterprises."[27] Only some of Professor Ostrom's design principles, though, are applicable in the Internet of Everything and are discussed in turn.[28]

A. *Defined Boundaries*

According to Professor Ostrom, "the boundary rules relate to who can enter, harvest, manage, and potentially exclude others' impacts. Participants then have more assurance about trustworthiness and cooperation of the others involved."[29] In the IoE context, defined boundaries are problematic given the extent to which various smart devices interconnect, forming "smart homes" and eventually "smart cities" that may be conceptualized as an ecosystem with its final realization in an Internet of Everything.[30] Trust, then, may only be built in such a landscape by segmenting the IoE into smaller micro communities, and/or by leveraging new technologies, such as

[18] *Id.* at 47.
[19] *See* ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION 212 (1990).
[20] SUSAN J. BUCK, THE GLOBAL COMMONS: AN INTRODUCTION 32 (1998).
[21] *See* OSTROM, *supra* note 19, at 90.
[22] BUCK, *supra* note 20, at 32.
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] Elinor Ostrom, *Polycentric Systems: Multilevel Governance Involving a Diversity of Organizations*, *in* GLOBAL ENVIRONMENTAL COMMONS: ANALYTICAL AND POLITICAL CHALLENGES INVOLVING A DIVERSITY OF ORGANIZATIONS 105, 118 tbl. 5.3 (Eric Brousseau et al. eds., 2012).
[27] *Id.*
[28] An earlier version of this research appeared as Shackelford et al., *supra* note 13.
[29] *Id.* at 464.
[30] *See, e.g.*, Abdullahi Arabo, *Cyber Security Challenges within the Connected Home Ecosystem Futures*, 61 PROCEDIA COMP. SCI. 227, 227 (2015).

blockchain, as is discussed further below.[31]

B. *Proportionality*

A key component of proportionality is equity, such that some of the "users [do not] get all the benefits and pay few of the costs . . . ."[32] Problems of proportionality often arise in the cybersecurity context, given well-documented issues with misaligned incentive structures.[33] For example, the National Bureau of Economic Research has estimated that the average firm only sees an approximately one percent drop in stock value following a cyber attack, though the figure raises to six percent for firms with insufficiently engaged Boards of Directors.[34] Under this argument, cybersecurity may be considered as a public good alongside national security, and if cyber attacks do not result in increased cybersecurity investments, then there exists a market failure in the IoE context, necessitating some form of regulatory intervention to correct, as is discussed further below.[35]

C. *Collective-Choice Arrangements and Minimal Recognition of Rights*

Good governance of common-pool resources may be reinforced when "most of the individuals affected by a resource regime are authorized to participate in making and modifying the rules related to

---

[31] Dep't Homeland Sec., *Information Sharing and Analysis Organizations (ISAOs)*, http://www.dhs.gov/isao (last visited Dec. 17, 2015).

[32] Ostrom, *supra* note 26, at 120.

[33] *See* Intel., *New Global Cybersecurity Report Reveals Misaligned Incentives, Executive Overconfidence Create Advantages for Attacker*, PHYS.ORG (Mar. 1, 2017), https://phys.org/news/2017-03-global-cybersecurity-reveals-misaligned-incentives.html.

[34] René M. Stulz, *What is the Impact of Successful Cyberattacks on Target Firms?*, HARV. L.F. ON CORP. GOVERNANCE & FIN. REG., (Mar. 30, 2018), https://corpgov.law.harvard.edu/2018/03/30/what-is-the-impact-of-successful-cyberattacks-on-target-firms/ ("We find a significant negative abnormal return for firms that announce a cyberattack. In particular, for firms experiencing cyberattacks that result in loss of personal financial information such as social security numbers, bank account, and credit card information, their mean cumulative abnormal returns from one day before to one day after the cyberattack announcement date is -1.12%, which implies an average value loss of $607 million. Cyberattacks have a much worse impact when the incident is a recurring event within one year and when affected firms are older. The impact is especially negative when the affected firm does not have evidence of board attention to risk management as the abnormal return is lower by 6 percentage points for such a firm.").

[35] *See* Robert Beeres & Myriame Bollen, *An Economic Analysis of Cyber Attacks*, *in* CYBER WARFARE: CRITICAL PERSPECTIVES 147, 153 (Paul Ducheine et al. eds., 2012) (discussing cyber security as a public good and, thus, defining it as "the goods, services, measures, techniques that aim to enhance the feeling of being secure in cyberspace"); Eli Dourado, *Is There a Cybersecurity Market Failure?* (George Mason Univ. Mercatus Ctr., Working Paper No. 12–05, 2012), http://mercatus.org/publication/there-cybersecurity-market-failure-0 (arguing that market failures are not so common in the cybersecurity realm); Jennifer Booton, *3 Reasons Why Cyberattacks Don't Hurt Stock Prices*, MARKETWATCH (Apr. 3, 2015, 1:33 PM), http://www.marketwatch.com/story/3-reasons-why-cyberattacks-dont-hurt-stock-prices-2015-04-03.

boundaries, assessment of costs . . . . etc."[36] Such an outcome, though, is not foreordained in most governance systems, given that it requires engaged and proactive rulemaking by technical communities (such as the Internet Engineering Task Force), the private sector, and the international community.[37] Such efforts have been on display in the IoE context, as seen in the National Institute for Standards and Technology Cybersecurity Framework (NIST CSF) and related NIST Privacy Framework, along with the Paris Call for Trust and Security in Cyberspace, which are analyzed further in Part III(C).[38]

D. *Monitoring*

Trust is a necessary but insufficient criterion to promote good governance, according to the literature on polycentric governance.[39] Monitoring is also vital to ensure "conformance of others to local rules."[40] Norm entrepreneurs, such as Microsoft, could fill this role. Already, we are seeing the beginning of this trend through the more than sixty participants in the Cybersecurity Tech Accord, which seeks to set out industry norms barring covered firms from using their platforms and tools to attack civilian critical infrastructure.[41] This role could also be fulfilled by the courts through litigation such as *LabMD, Inc. v. FTC*, along with other state and federal actions, which are forming the contours of what constitutes a "reasonable" level of cybersecurity care for IoE operators.[42]

E. *Graduated Sanctions and Dispute Resolution*

The Design Principles also underscore the need for graduated sanctions and effective dispute resolution for rule breakers. The former point underscores the significance of not "[l]etting an infraction pass

---

36 Ostrom, *supra* note 26, at 120.

37 *See* George J. Siedel & Helena Haapio, *Using Proactive Law for Competitive Advantage*, 47 AM. BUS. L.J. 641, 656–57 (2010) (discussing the origins of the proactive law movement, which may be considered "a future-oriented approach to law placing an emphasis on legal knowledge to be applied before things go wrong").

38 Press Release, NIST, NIST Releases Version 1.1 of Its Popular Cybersecurity Framework (Apr. 16, 2018) (available at https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework); *Privacy Framework*, NIST, https://www.nist.gov/privacy-framework (last visited Jan. 9, 2018).

39 Ostrom, *supra* note 26, at 120.

40 *Id*. at 121.

41 *See* CYBERSECURITY TECH ACCORD, https://cybertechaccord.org/ (last visited Oct. 3, 2018).

42 *See* Allison Frankel, *There's a Big Problem for the FTC Lurking in the 11th Circuit's LabMD Data-Security Ruling*, REUTERS (June 7, 2018), https://www.reuters.com/article/us-otc-labmd/theres-a-big-problem-for-the-ftc-lurking-in-11th-circuits-labmd-data-security-ruling-idUSKCN1J32S2; *see also* Scott J. Shackelford, Scott Russell & Jeffrey Haut, *Bottoms Up: A Comparison of "Voluntary" Cybersecurity Frameworks*, 16 UNIV. CAL. DAVIS BUS. L.J. 217 (2016).

unnoticed."[43] There have also been proposals, especially in the wake of scandals such as the October 2018 Facebook data breach, to increase penalties and resources at the federal level, such as through stepped-up Federal Trade Commission (FTC) enforcement.[44]

F. *Summary*

Together, these Design Principles provide some guidance for the governance of the Internet of Everything, such as the importance of graduated sanctions and encouraging bottom-up efforts for the NIST CSF and the Cybersecurity Tech Accord. By following the insights of these Principles, it may be possible to promote the sustainable development of these technologies, even though such conceptions are often divorced from normative stances. As Professor Cole has asserted, "we might legitimately argue that the 'design principles' from Governing the Commons were informed by an implicit normative commitment to long-run sustainability."[45] The full picture, though, requires a deeper dive into the IAD and GKC Frameworks, discussed next.

III. 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.[46] "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,"[47] cybersecurity, and Internet governance. Without some level of clarity, according to Cole, confusion can occur, such as in defining "resource systems" that can include "information, data, or knowledge" in the intellectual property context, with natural resources.[48] Similarly, CPRs may refer to common-pool resources (e.g., "naturally existing systems with various biophysical attributes") and common-property regimes (e.g., "human-created sets of institutions for managing common-pool resources.").[49] In

[43] *See* Ostrom, *supra* note 26, at 121.
[44] *See*, *e.g.*, Emily Bary, *Facebook Could Face Huge Fines in FTC Investigation*, MARKET WATCH (Mar. 26, 2018), https://www.marketwatch.com/story/facebook-could-face-huge-fines-in-ftc-investigation-2018-03-26; s*ee also* Alex Hickey, *'Punching Above its Weight,' FTC Needs More Rule-Making Power, Resources, Commissioner Says*, CIO DIVE (Oct. 3, 2018), https://www.ciodive.com/news/punching-above-its-weight-ftc-needs-more-rule-making-power-resources-c/538718/.
[45] Cole, *supra* note 14, at 49.
[46] *Id*. at 50–51.
[47] *Id.* at 51.
[48] *Id*.
[49] *Id*. at 52.

the Internet governance context, similar confusion surrounds core terms such as "information security" and "cybersecurity."[50] 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.[51] 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."[52]

Although created for a different context, the IAD Framework can nevertheless (a) improve our "understanding of information and information flows under alternative institutional arrangements; (b) diagnose problems (or dilemmas) in existing institutional arrangements; and (c) predict[, in select cases, the] outcomes under alternative institutional arrangements."[53] Indeed, Professor Ostrom believed that the IAD Framework had wide application, including, "to microeconomic theory, game theory, transaction cost theory, social cost theory, public choice, and constitutional and covenantal theory, along with theories of public goods and common-pool resources."[54] It is now arguably "the most widely used framework in studies of the natural commons."[55] The IAD Framework is unpacked in Figure 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.

[50] *See* Neal Ungerleider, *The Chinese Way of Hacking*, FAST CO., (July 12, 2011), http://www.fastcompany.com/1766812/inside-the-chinese-way-of-hacking (transcribing an interview with Adam Segal, the Ira A. Lipman Fellow at the Council on Foreign Relations, in which Mr. Segal discusses how the Chinese differentiate between information security and cybersecurity).

[51] *See* Scott J. Shackelford, Scott Russell & Andreas Kuehn, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. INT'L L. 1 (2016); Scott J. Shackelford & Amanda N. Craig, *Beyond the New 'Digital Divide': Analyzing the Evolving Role of Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119 (2014).

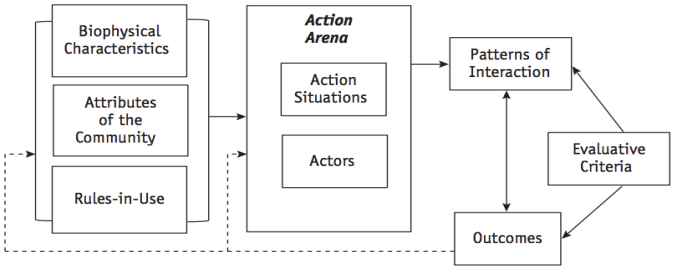
[52] Cole, *supra* note 14, at 52.

[53] *Id*. at 46.

[54] *Id*. at 49.

[55] *Id*. at 52.

Figure 1: The Institutional Analysis and Development (IAD) Framework[56]



A. *Biophysical Characteristics and Classifying Goods in Cyberspace*

Digging into the IAD Framework, beginning on the left side of Figure 1 (with all three boxes being considered as endogenous variables to the Framework),[57] 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."[58] 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.[59] Internet governance institutions (or "facilities" in this vernacular) can also control the rate at which ideas are diffused, such as through censorship.[60]

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.[61] Exclusion refers to the relative ease with which goods may be protected.[62] Subtractability evokes the extent to which one's use of a good decreases another's enjoyment of it.[63] 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

---

[56] Elinor Ostrom & Charlotte Hess, *A Framework for Analyzing the Knowledge Commons*, in UNDERSTANDING KNOWLEDGE AS A COMMONS: FROM THEORY TO PRACTICE 44, fig. 3.1 (Charlotte Hess & E. Ostrom eds., 2007).

[57] *Id*. at 9.

[58] *Id*. at 10.

[59] For more on this topic, see Scott J. Shackelford et al., *Using BITs to Protect Bytes: Promoting Cyber Peace and Safeguarding Trade Secrets through Bilateral Investment Treaties*, 52 AM. BUS. L.J. 1 (2015).

[60] *See, e.g.*, Hannah Beech, *China's Great Firewall is Harming Innovation, Scholars Say*, TIME (June 2, 2016), http://time.com/4354665/china-great-firewall-innovation-online-censorship/.

[61] SUSAN J. BUCK, THE GLOBAL COMMONS: AN INTRODUCTION 5–6 (1998).

[62] *Id.*

[63] *See id.*

"private goods" that are defined by property law and best regulated by the market.[64] Examples range from iPads to toy cars. 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.[65] An example is national defense, including, some argue, cybersecurity.[66] But, in its totality, the Internet of Everything includes all forms of goods, including devices catalyzing a range of positive and negative externalities, from network effects to cyber-attacks. The Internet of Everything 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.[67] Such communal property rights may either be recognized by the state, or be based on "benign neglect."[68] Indeed, as of this writing, there is an active debate underway in the U.S. and Europe about the regulation of social-media platforms to limit the spread of terrorist propaganda, junk news, sex trafficking, and hate speech.[69] Such mixed types of goods are more the norm than the exception. As Cole has argued,

> since 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.'[70]

Naturally, the next question is whether, in fact, cyberspace may be comparable to the atmosphere as an *impure* public good, since *pure*

---

[64] *See id.* For an extended treatment of this subject, see Janine Hiller & Scott J. Shackelford, *The Firm and Common Pool Resource Theory: Unpacking the Rise of Benefit Corporations*, 55 AM. BUS. L.J. 5 (2018).

[65] *See* Vincent Ostrom & Elinor Ostrom, *Public Goods and Public Choices*, *in* ELINOR OSTROM AND THE BLOOMINGTON SCHOOL OF POLITICAL ECONOMY Vol. 2, at 3, 6 (Daniel H. Cole & Michael McGinnis eds., 2015).

[66] ELINOR OSTROM, BEYOND MARKETS AND STATES: POLYCENTRIC GOVERNANCE OF COMPLEX ECONOMIC SYSTEMS 413 (2009), http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/2009/ostrom_lecture.pdf (2009 Nobel Prize lecture).

[67] *See* Kevin Roose, *Reddit Limits Noxious Content by Giving Trolls Fewer Places to Gather*, N.Y. TIMES (Sept. 25, 2017), https://www.nytimes.com/2017/09/25/business/reddit-limits-noxious-content-by-giving-trolls-fewer-places-to-gather.html.

[68] BUCK, *supra* note 61, at 5.

[69] *See, e.g.*, *SESTA Is Flawed, but the Debate Over It Is Welcome*, ECONOMIST (Sept. 23, 2017), https://www.economist.com/leaders/2017/09/23/sesta-is-flawed-but-the-debate-over-it-is-welcome (discussing the extent to which legal liability should attach to online services that have long enjoyed immunity in the U.S. under the Communications Decency Act).

[70] Cole, *supra* note 14, at 54.

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 all common pool resources.[71] Though cyberspace is unique given that it can, in fact, expand such as through the addition of new networks,[72] but increased use also multiplies threat vectors.[73]

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."[74] However, in practice, as Elinor Ostrom and numerous others have shown,[75] self-organization is in fact possible in practice, as is discussed further below. Without such polycentric action, this vital, digital common-pool resource may be depleted.[76] The growth of the Internet of Everything could hasten such tragedies if vulnerabilities replete in this ecosystem are allowed to go unaddressed.[77]

B. *Community Attributes*

The next box on the left side of the IAD Framework, titled

---

[71] *See* David Feeny et al., *The Tragedy of the Commons: Twenty-Two Years Later*, 18 HUM. ECOLOGY 1, 4 (1990). Former DHS Secretary Michael Chertoff, for example, has argued that the cyber threat constitutes "a potential tragedy of the commons scenario," given "[o]ur reliance on cyberspace." Michael Chertoff, *Foreword*, 4 J. NAT'L SEC. L. & POL'Y 1, 2 (2010).

[72] *See* TIM JORDAN, CYBERPOWER: THE CULTURE AND POLITICS OF CYBERSPACE AND THE INTERNET 120 (1999) (describing the increase in Internet access as well as information overload); *cf*. RON DEIBERT, DISTRIBUTED SECURITY AS CYBER STRATEGY: OUTLINING A COMPREHENSIVE APPROACH FOR CANADA IN CYBERSPACE 6–11 (2012), https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf (discussing the expansion of cyberspace to other countries and regions of the world, yet noting the increasing use of censorship practices within some of these nations).

[73] *See* Nick Nykodym et al., *Criminal Profiling and Insider Cyber Crime*, 2 DIGITAL INVESTIGATION 261, 264–65 (2005) (explaining how the Internet's expanding role in business has correspondingly increased the threat of cybercrime and made criminals more difficult to catch); Richard Chirgwin, *AusCERT Wrap-Up, Day 2: Attack Vectors Will Multiply Faster than Defenses*, CSO (May 17, 2012), http://www.cso.com.au/article/424868/auscert_wrap-up_day_2_attack_vectors_will_multiply_faster_than_defences/ (declaring that it is "hard to escape the conclusion that the 'Internet of Things' will create a host of new attack vectors that will probably only become clear after we have enthusiastically adopted a new technology").

[74] Brett M. Frischmann, Michael J. Madison & Katherine J. Strandburg, *Governing Knowledge Commons*, *in* GOVERNING KNOWLEDGE COMMONS 1, 54 (Brett M. Frischmann, Michael J. Madison & Katherine J. Strandburg eds., 2014)

[75] *See, e.g.*, Brett Frischmann, *The Tragedy of the Commons, Revisited*, SCI. AM.: OBSERVATIONS. (Nov. 19, 2018), https://blogs.scientificamerican.com/observations/the-tragedy-of-the-commons-revisited.

[76] *See, e.g.*, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, EUR. COMM'N, at 2 (Feb. 7, 2013) (reporting that "a 2012 Eurobarometer survey showed that almost a third of Europeans are not confident in their ability to use the internet for banking or purchases") [hereinafter *EU Cybersecurity Strategy*].

[77] *See, e.g.*, Michael Smith, '*The Tragedy of the Commons' in the IoT Ecosystem*, COMPUTERWORLD (Aug. 16, 2017, 9:32 AM), https://www.computerworld.com.au/article/626059/tragedy-commons-iot-ecosystem/.

"Attributes of the Community," refers to the network of users making use of the given resource.[78] Unlike in the natural commons context in which relatively small, local communities might share access to a forest or lake, in the cyber context, communities can be far larger given the more than four billion global Internet users as of October 2018,[79] not to mention the billions of devices comprising the Internet of Everything. The scale of the problem parallels the battle to combat the worst effects of global climate change.[80] Such a vast scale stretches the utility of the IAD Framework, which is why most efforts have considered subparts, or clubs, within this ecosystem.

An array of polycentric theorists, including Professor Ostrom, have extolled the benefits of small, self-organized communities in managing common pool resources.[81] Anthropological evidence has confirmed the benefits of small-scale governance.[82] However, micro-communities can ignore other interests, as well as the wider impact of their actions.[83] Sustainable development, such as corporate social responsibility tools like the Global Reporting Initiative, are a useful mechanism for overcoming these issues.[84] A polycentric model favoring bottom-up governance but with a role for centralized coordination so as to protect against free riders may be the best-case scenario.[85] Such self-regulation has the flexibility "to adapt to rapid technological progress"[86] better

[78] Cole, *supra* note 14, at 55.

[79] *See* INTERNET WORLD STATS, https://www.internetworldstats.com/stats.htm (last visited Oct. 2, 2018).

[80] Cole, *supra* note 14, at 56. For an analysis of how the Ostrom Design Principles might apply in this context, see Scott J. Shackelford, *On Climate Change and Cyber Attacks: Leveraging Polycentric Governance to Mitigate Global Collective Action Problems*, 18 VAND. J. ENT. & TECH. L. 653 (2016) (analyzing how the Ostrom Design Principles might apply in this context.).

[81] *See, e.g.*, Elinor Ostrom et al., *Revisiting the Commons: Local Lessons, Global Challenges*, 284 SCI. 278, 278 (1999) (questioning policymakers' use of Garrett Hardin's theory of the "tragedy of the commons," in light of the empirical data showing self-organizing groups can communally manage common-pool resources).

[82] *See, e.g.*, Gregory A. Johnson, *Organizational Structure and Scalar Stress*, *in* THEORY AND EXPLANATION IN ARCHEOLOGY 389, 392–94 (Colin Renfrew et al. eds., 1982).

[83] *See* ANDREW D. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 164 (2007) (explaining how members of micro-communities tend to focus only on what directly impacts their own activities).

[84] *See* Scott J. Shackelford et al., *Sustainable Cybersecurity: Applying Lessons from the Green Movement to Managing Cyber Attacks*, 2016 UNIV. ILL. L. REV. 1995 (2016).

[85] The DHS's Cybersecurity Awareness Month every October helps to highlight the important role played by bottom-up efforts to enhance cybersecurity, noting, "[e]very Internet user has a role to play in securing cyberspace and ensuring the safety of ourselves, our families, and our *communities online*." *National Cyber Security Awareness Month*, DEP'T HOMELAND SEC., http://www.dhs.gov/national-cyber-security-awareness-month (last visited Jan. 24, 2013). Competitions rewarding communities that distinguish themselves in enhancing their cybersecurity along defined metrics such as through grants could also help build awareness and increase the potential for successful polycentric governance, especially when coupled with other hallmarks such as effective dispute resolution.

[86] According to Notre Dame Professor Don Howard, different online communities "have a complicated topology and geography, with overlap, hierarchy, varying degrees of mutual

than black letter law, which often changes incrementally, if at all. Even if enacted, it 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."[87]

C. *Rules-in-Use*

This component of the IAD Framework comprises both community norms along with formal legal rules.[88] 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.[89] The driving research task in this variable, according to Cole, "in applying the IAD framework, is to determine, and diagnose perceived problems with, the rules-in-use that govern day-to-day ('operational-level') interactions in the action situations under study."[90] 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[91] and the Carnegie Endowment International Cybersecurity Norms Project, but such efforts remain at an early stage of development.[92] A variety of

isolation and mutual interaction. There are also communities of corporations or corporate persons, gangs of thieves, and . . . on scales small and large." Don Howard, *Civic Virtue and Cybersecurity*, *in* THE NATURE OF PEACE AND THE MORALITY OF ARMED CONFLICT 192 (Florian Demont-Biaggi ed., 2017). What is more, Professor Howard argues that these communities will each construct norms in their own ways, and at their own rates, but that this process has the potential to make positive progress toward addressing multifaceted issues such as enhancing cybersecurity. *Id*. at 199. For more on this topic, see SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE, ch.7 (2014).

87 Adi Robertson, *California Just Became the First State with an Internet of Things Cybersecurity Law*, VERGE (Sept. 28, 2018, 6:07 PM), https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law.

88 Cole, *supra* note 14, at 56.

89 *Id*. at 57.

90 *Id*.

91 INT'L TELECOMM. UNION, GLOBAL CYBERSECURITY INDEX (2017) (available at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf).

92 *See Cyber Norms Index*, CARNEGIE ENDOWMENT FOR INT'L PEACE, https://carnegieendowment.org/publications/interactive/cybernorms (last visited Oct. 2, 2018).

rules may be considered to help address governance gaps, such as "position rules," as is discussed further in Figure 2.

Figure 2: Types of Rules[93]

Position rules	Define positions that actors hold, including as owners of property rights and duties.
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;
	(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.
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.
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.

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.[94]

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 U.S. privacy protections. Although not comparable to the EU's new General Data Protection Regulation (GDPR) discussed below, 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.[95] Whether such state-level action, even in a state with an

[93] Elinor Ostrom & Sue Crawford, *Classifying Rules*, *in* UNDERSTANDING INSTITUTIONAL DIVERSITY 186 (Elinor Ostrom ed., 2005).

[94] *See, e.g.*, Marguerite Reardon, *Facebook's FTC Consent Decree Deal: What You Need to Know*, CNET (Apr. 14, 2018), https://www.cnet.com/news/facebooks-ftc-consent-decree-deal-what-you-need-to-know.

[95] *See* Ben Adler, *California Passes Strict Internet Privacy Law with Implications for The Country*, NAT'L PUB. RADIO (June 29, 2018, 5:05 AM), https://www.npr.org/2018/06/29/624336039/california-passes-strict-internet-privacy-law-with-implications-for-the-country.

economic footprint the size of California, will help foster enhanced cybersecurity due diligence across the broader IoE ecosystem remains to be seen.

D. *Action Arenas*

The arena is just that, the place where decisions are made, where "collective action succeeds or fails."[96] Such arenas exist at three levels within the IAD Framework—constitutional, collective-choice, and operational.[97] Decisions made at each of these governance levels, in turn, impact a range of rules and community attributes, which is an important feature of the Framework that makes it "uniquely compatible with multiple theories and models, including . . . neoclassical theory, game theory, public choice theory, and behavioral economics, with the exception of (usually deterministic) models of irrational behavior."[98] Examples of decisionmakers in each arena in the cybersecurity context include (1) at the constitutional level, judges deciding the bounds of "reasonable care" and "due diligence";[99] (2) federal and state policymakers at the collective-choice (e.g., policy) level, such as FCC Commissioners deciding the bounds of net neutrality (although a case can be made there for them being at the constitutional level); and (3) at the operational level, firms and everyone else.[100]

E. *Outcomes*

This component of the IAD Framework references predictable outcomes of interactions from social situations, which can include consequences for both resource systems and units.[101] Whether such outcomes are positive or negative is a normative question. 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,"[102] 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 Galtung described the new field of

96 Cole, *supra* note 14, at 59.
97 *Id.*
98 *Id.*
99 *See* Scott J. Shackelford et al., *Toward a Global Standard of Cybersecurity Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 287 (2015).
100 Cole, *supra* note 14, at 60.
101 *Id.* at 61.
102 *Digital Peace Now*, MICROSOFT, https://digitalpeace.microsoft.com/ (last visited Nov. 5, 2018).

peace studies he helped create in 1969.[103] 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.[104] 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."[105] Cyber peace is defined here not as the absence of conflict, what may be called negative cyber peace.[106] 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 below, 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.[107] 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."[108] Such a polycentric approach is also a necessity in the cyber regime

103 Johan Galtung, *Violence, Peace, and Peace Research*, 6 J. PEACE RES. 167, 168 (1969).

104 *Id.*

105 *Id.*

106 The notion of negative peace has been applied in diverse contexts, including civil rights. *See, e.g.*, Martin Luther King, Jr., *Non-Violence and Racial Justice*, CHRISTIAN CENTURY, Feb. 6, 1957, at 118, 119 (arguing "[t]rue peace is not merely the absence of some negative force—tension, confusion or war; it is the presence of some positive force—justice, good will and brotherhood.").

107 *See* Johan Galtung, *Peace, Positive and Negative*, *in* THE ENCYCLOPEDIA OF PEACE PSYCHOLOGY 758–60 (Daniel J. Christie ed., 2012) (comparing the concepts of negative and positive peace). Definitions of positive peace vary depending on context, but the overarching issue in the cybersecurity space is the need to address structural problems in all forms, including the root causes of cyber insecurity such as economic and political inequities, legal ambiguities, as well as working to build a culture of peace. *Id.* at 759. ("The goal is to build a structure based on reciprocity, equal rights, benefits, and dignity . . . and a culture of peace, confirming and stimulating an equitable economy and an equal polity."); *see also* G.A. Res. 53/243A, Declaration on a Culture of Peace (Oct. 6, 1999) (offering a discussion of the prerequisites for creating a culture of peace including education, multi-stakeholder collaboration, and the "promotion of the rights of everyone to freedom of expression, opinion and information").

108 Cole, *supra* note 14, at 61.

complex, given the prevalence of private and public sector stakeholder controls.

F. *Evaluative Criteria*

The final IAD framework box, according to Cole, is "the most neglected and underdeveloped" of the frameworks.[109] 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."[110] 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."[111] 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."[112]

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. According to Frank Montoya, the former U.S. National Counterintelligence Chief, "[w]e're an information-based society now. Information is everything. That makes . . . company executives, the front line—not the support mechanism, the front line—in [determining] what comes."[113] This means the role of the private sector is integral in ongoing efforts aimed at enhancing cybersecurity in the Internet of Everything, much like the increasingly vital role firms are playing in fostering sustainability.[114] Similar trends are playing out in cybersecurity circles,[115] which are prompting the consideration of novel cybersecurity strategies aimed at translating this increased interest into action, including certification schemes inspired by the organic trade movement, and even the application of environmental law principles such as "no harm" to help

109 *Id.* at 62.
110 *Id.* at 62.
111 Hess & Ostrom, *supra* note 56, at 62.
112 Cole, *supra* note 14, at 62.
113 Tom Gjelten, *Bill Would Have Businesses Foot Cost of Cyberwar*, NAT'L PUB. RADIO (May 8, 2012), http://www.npr.org/2012/05/08/152219617/bill-would-have-businesses-foot-cost-of-cyber-war.
114 *See A New Era of Sustainability: UN Global Compact–Accenture CEO Study 2010*, UNITED NATIONS GLOBAL COMPACT (June 2010), https://www.unglobalcompact.org/docs/news_events/8.1/UNGC_Accenture_CEO_Study_2010.pdf.
115 *See, e.g.*, Matt Egan, *Survey: Investors Crave More Cyber Security Transparency*, FOX BUS. (Mar. 4, 2013), https://www.foxbusiness.com/markets/survey-investors-crave-more-cyber-security-transparency.

fill out an international cybersecurity due diligence norm.[116] 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 Internet of Everything. Such an approach also accords with the "environmental metaphor for information law and policy" that has been helpful in other efforts.[117] However, the analogy is not perfect, given that, unlike in the natural world, "knowledge commons arrangements usually must create a governance structure within which participants not only share existing resources but also engage in producing those resources and, indeed, in determining their character."[118]

G. *Summary and GKC Insights*

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. Given these distinctions, Professor Brett Frischmann has suggested a revised IAD Framework for the Knowledge Commons reproduced in Figure 3.

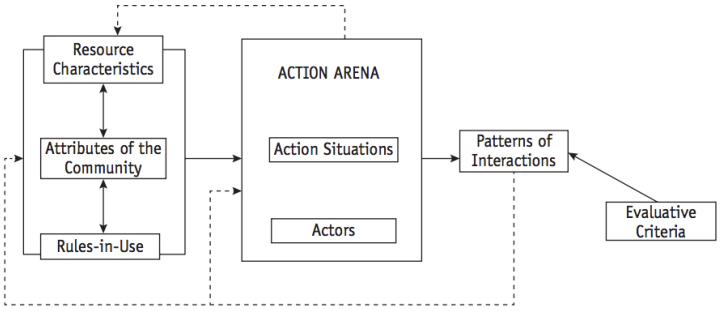


Figure 3: Governing Knowledge Commons Framework[119]

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. 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

116 *See* Shackelford et al., *supra* note 84.
117 Frischmann, Madison & Strandburg, *supra* note 74, at 16.
118 *Id.*
119 *Id.* at 19.

knowledge commons are often inseparable.[120] These insights also resonate in the IoE context, given the tremendous amount of interactions between stakeholders, including IoT device manufactures, 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 context, as seen in the Mirai botnet, in which compromised smart light bulbs were networked to crash critical Internet services.[121]

An array of research questions can and should be pursued using the GKC Framework as applied to the IoE, as are laid out in Figure 4.

Figure 4: Knowledge Commons Framework and Representative Research Questions[122]

Background Environment	
	• What is the background context (legal, cultural, etc.) of this particular commons?
	• What normative values are relevant for this community?
	• What is the "default" status of the resources involved in the commons (patented, copyrighted, open, or other)?
	• How does this community fit into a larger context? What relevant domains overlap in this context?
Attributes	
Resources	• What resources are pooled and how are they created or obtained?
	• What are the characteristics of the resources? Are they rival or nonrival, tangible or intangible? Is there shared infrastructure?
	• What is personal information relative to resources in this

120 *Id.*

121 *See* Bogdan Botezatu, *Unprotected IoT Devices Killed the US Internet for Hours*, BITDEFENDER (Oct. 23, 2016), https://www.bitdefender.com/box/blog/iot-news/mirai-iot-security-alert/.

122 Frischmann, Madison & Strandburg, *supra* note 74, at 20–21.

	action arena?
	• What technologies and skills are needed to create, obtain, maintain, and use the resources?
	• What are considered to be appropriate resource flows? How is appropriateness of resource use structured or protected?
Community Members	• Who are the community members and what are their roles?
	• What are the degree and nature of openness with respect to each type of community member and the general public?
	• What non-community members are impacted?
Goals and Objectives	• What are the goals and objectives of the commons and its members, including obstacles or dilemmas to be overcome?
	• Who determines goals and objectives?
	• What values are reflected in goals and objectives?
	• What are the history and narrative of the commons?
	• What is the value of knowledge production in this context?
Governance	
Context	• What are the relevant action arenas? How do they relate to the goals and objectives of the commons and the relationships among various types of participants, and with the general public?
	• Are action arenas perceived to be legitimate?
Institutions	• What legal structures (e.g., intellectual property, subsidies, contract, licensing, tax, antitrust) apply?

	• What are the governance mechanisms (e.g., membership rules, resource contribution or extraction standards and requirements, conflict resolution mechanisms, sanctions for rule violation)?
	• What are the institutions and technological infrastructures that structure and govern decision making?
	• What informal norms govern the commons?
	• What institutions are perceived to be legitimate? Illegitimate? How are institutional illegitimacies addressed?
Actors	• Who are the decision-makers, and how are they selected? Are decision-makers perceived to be legitimate?
	• How do nonmembers interact with the commons? What institutions govern those interactions?
	• Are there impacted groups that have no say in governance?
Patterns and Outcomes	
	• What benefits are delivered to members and to others (e.g., innovations and creative output, production, sharing, and dissemination to a broader audience, and social interactions that emerge from the commons)?
	• What costs and risks are associated with the commons, including any negative externalities?
	• Are outcomes perceived to be legitimate by members? By decision-makers? By impacted outsiders?

Space constraints prohibit a comprehensive analysis of how each of these questions apply in the IoE context, and many of these points were addressed already in reference to the Ostrom Design Principles, as well as the IAD and GKC Frameworks. In brief, though, and focusing on the governance section, as has been discussed in reference to action arenas, there are a huge number of forums—both public and private—in play, including sector-specific ISACs, broader Information Sharing and

Analysis Organizations (ISAOs), as well as Cyber Emergency Response Teams (CERTs) and joint Security Operations Centers (SOCs). It is important to recognize the polycentric nature of this domain 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).[123] 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),[124] 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 below after first considering the application of blockchain tech to build trust in the distributed IoE.

IV. IS BLOCKCHAIN THE ANSWER TO THE IOE'S WOES?

Professor Ostrom argued that "[t]rust is the most important resource."[125] 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 IAD and GKC Frameworks provide useful insights toward this end. But one technology could also help in this effort, namely blockchain,[126] which, according to Goldman Sachs, could "change 'everything.'"[127] Regardless of the question being asked, some argue that it is the answer to the uninitiated—namely, a blockchain cryptographic distributed ledger.[128] Its applications are widespread, from recording property deeds

123 *See* Scott J. Shackelford & Amanda N. Craig, *Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119, 119 (2014).

124 *Id.*

125 *Interview with Nobel Laureate Elinor Ostrom*, ESCOTET FOUND., http://escotet.org/2010/11/interview-with-nobel-laureate-elinor-ostrom/ (last visited June 29, 2018).

126 *See* Naomi Lachance, *Not Just Bitcoin: Why the Blockchain Is a Seductive Technology to Many Industries*, NAT'L PUB. RADIO (May 4, 2016, 7:01 AM), http://www.npr.org/sections/alltechconsidered/2016/05/04/476597296/not-just-Bitcoin-why-blockchain-is-a-seductive-technology-to-many-industries.

127 *Id.*

128 At its root, a blockchain is a "shared, trusted, public ledger that everyone can inspect, but which no single user controls." *The Promise of the Blockchain: The Trust Machine*, ECONOMIST (Oct. 31, 2015), https://www.economist.com/leaders/2015/10/31/the-trust-machine. For more on how blockchain works, see Appendix A in Scott J. Shackelford & Steve Myers, *Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace*, 19

to securing medical devices.[129] As such, its potential is being investigated by a huge range of organizations.[130] These include the U.S. Defense Advanced Research Projects Agency (DARPA),[131] IBM, Maersk, Disney,[132] 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.[133] Examples are similarly abound regarding how firms use blockchains to enhance cybersecurity.[134] The technology could enable the Internet to become decentralized, pushing back against the type of closed platforms analyzed by Professor Johnathan Zittrain and others,[135] but this "will only happen when it becomes accepted that decentralized is safer than centralized."[136] 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.[137]

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.[138] But the potential for progress demands further research,

YALE J.L. & TECH. 334, 383–88 (2017).

129 *See* Asha McLean, *ASX Argues Medical Records Are Ripe for Blockchain*, ZDNET (Nov. 16, 2016), http://www.zdnet.com/article/asx-argues-medical-records-are-ripe-for-blockchain/. *See generally* Scott J. Shackelford et al., *Securing the Internet of Healthcare*, 19 MINN. J.L. SCI. & TECH. 405 (2018).

130 *See* Kyle Torpey, *Prediction: $10 Billion Will Be Invested in Blockchain Projects in 2016*, COIN J. (Jan. 22, 2016), http://coinjournal.net/prediction-10-billion-will-be-invested-in-blockchain-startups-in-2016/.

131 *See* Lachance, *supra* note 126.

132 *See* Don Tapscott & Alex Tapscott, *Here's Why Blockchains Will Change the World*, FORTUNE (May 8, 2016), http://fortune.com/2016/05/08/why-blockchains-will-change-the-world.

133 MICHAEL J. CASEY & PAUL VIGNA, THE TRUTH MACHINE: THE BLOCKCHAIN AND THE FUTURE OF EVERYTHING 6 (2018).

134 Tapscott & Tapscott, *supra* note 132.

135 JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 36–37 (2008).

136 Bernard Lunn, *Bitcoin Blockchain Could Solve the Cyber Security Challenge for Banks*, DAILY FINTECH (Oct. 30, 2015), https://dailyfintech.com/2015/10/30/Bitcoin-blockchain-could-solve-the-cyber-security-challenge-for-banks/.

137 *See* Adrian Zmudzinski, *Blockchain Adoption in IoT Industry More Than Doubled in 2018: Survey*, COINTELEGRAPH (Jan. 15, 2019), https://cointelegraph.com/news/blockchain-adoption-in-iot-industry-more-than-doubled-in-2018-survey.

138 *See* John Villasenor, *Blockchain Technology: Five Obstacles to Mainstream Adoption*, FORBES (June 3, 2018, 7:43 PM),

including how it could help promote a polycentric cyber peace in the burgeoning Internet of Everything.

V. POLYCENTRIC IMPLICATIONS FOR MANAGERS AND POLICYMAKERS

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.[139] Similar to the big questions in the field of intellectual property, such as defining the optimal duration of a copyright,[140] 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."[141]

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[142] that has been championed by numerous scholars, including Nobel Laureate, Elinor Ostrom, and Professor Vincent Ostrom.[143] It suggests that "a single governmental unit" is usually incapable of managing "global collective action problems"[144] such as cyber-attacks. Instead, a polycentric approach recognizes that diverse organizations working at multiple scales can enhance "flexibility across issues and adaptability over time."[145] Such

https://www.forbes.com/sites/johnvillasenor/2018/06/03/blockchain-technology-five-obstacles-to-mainstream-adoption/#6979b4955ad2.

139 Cole, *supra* note 14, at 46.

140 *Id.* at 47.

141 *Id.*

142 Michael D. McGinnis, *An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework*, 39 POL'Y STUD. J. 163, 171–72 (2011) (defining polycentricity as "a system of governance in which authorities from overlapping jurisdictions (or centers of authority) interact to determine the conditions under which these authorities, as well as the citizens subject to these jurisdictional units, are authorized to act as well as the constraints put upon their activities for public purposes").

143 Elinor Ostrom, *Polycentric Systems as One Approach for Solving Collective-Action Problems* 1 (Ind. Univ. Workshop in Pol. Theory & Pol'y Analysis, Working Paper Series No. 08–6, 2008), http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/4417/W08-6_Ostrom_DLC.pdf?sequence=1.

144 Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change* 35 (World Bank, Pol'y Res., Working Paper No. 5095, 2009), http://www.iadb.org/intal/intalcdi/pe/2009/04268.pdf.

145 Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change*, 9 PERSP. ON POL. 7, 15 (2011); *cf.* Julia Black, *Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes*, 2 REG. & GOVERNANCE 137, 157 (2008) (discussing the legitimacy of polycentric regimes, and arguing that "[a]ll regulatory regimes are polycentric to varying degrees . . . ").

an approach can help foster the emergence of a norm cascade improving the Security of Things.[146]

Not all polycentric systems are guaranteed to be successful. Disadvantages, for example, can include gridlock and a lack of defined hierarchy.[147] The Ostrom Design Principles can help predict the institutional success of given interventions,[148] then, but the literature remains immature, as does the current state of IoE governance. However, progress has been made on norm development, including cybersecurity due diligence, discussed below, which will help IoT manufacturers better fend off attacks against foreign nation states. Further polycentric efforts are needed, as was made evident when the Information Systems Audit and Control Association (ISACA)[149] surveyed IT professionals in the United Kingdom and found that "[seventy five] percent of the security experts polled say they do not believe device manufacturers are implementing sufficient security measures in IoT devices, and a further [seventy three] percent say existing security standards in the industry do not sufficiently address IoT *specific* security concerns."[150] Such sentiments are perhaps one reason that, according to a Dutch cybersecurity survey, "[seventy nine] percent [of respondents] are requesting more robust government-issued security guidelines."[151]

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."[152] 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."[153] In the IoE context, as has been noted, the scale could

146 *See* Martha Finnemore & Kathryn Sikkink, *International Norm Dynamics and Political Change*, 52 INT'L ORG. 887, 895–98 (1998). For a deeper dive on this topic, see Chapter 2 in SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE (2014).

147 *See* Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change* 17 (Harv. Project on Int'l Climate Agreements, Discussion Paper 10-33, 2010), http://belfercenter.ksg.harvard.edu/files/Keohane_Victor_Final_2.pdf.

148 For more on this topic, see Shackelford et al., *supra* note 13.

149 *See generally About ISACA*, ISACA, http://www.isaca.org/about-isaca/Pages/default.aspx (last visited Dec. 16, 2015) (stating that ISACA was previously known as "Information Systems Audit and Control Association").

150 *Existing Security Standards Do Not Sufficiently Address IoT*, HELP NET SEC. (Oct. 15, 2015), http://www.net-security.org/secworld.php?id=18981.

151 Zmudzinski, *supra* note 137.

152 Cole, *supra* note 14, at 47.

153 *Id.*

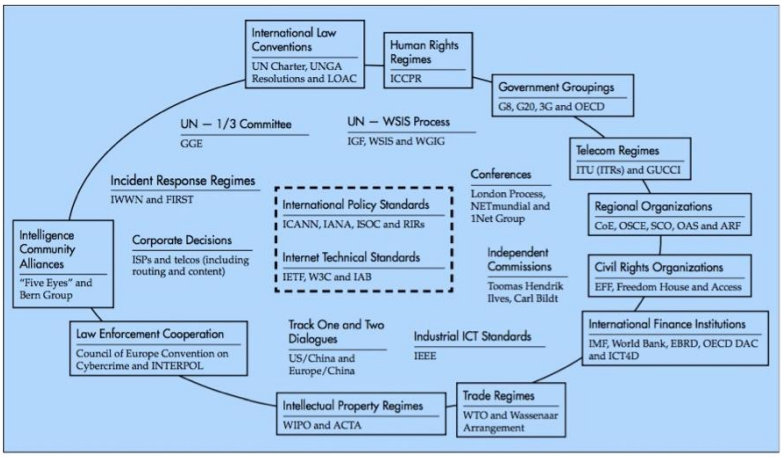
not be greater with billions of people and devices interacting across myriad sectors, settings, and societies. The sheer complexity of such a system, along with the history of Internet governance to date, signals that there can be no single solution or governance forum to foster cyber peace in the IoE. Rather, polycentric principles gleaned from the Ostrom Design Principles along with the IAD and GKC Frameworks 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 in the IoE. As has been noted, evaluation criteria are largely undefined in the IAD Framework, which the community should take as a call to action, such as by laying out the objectives of cyber peace in the Internet of Everything.[154] The members of the Cybersecurity Tech Accord and the Trusted IoT Alliance should take up this call to action and work with civil society, academics, and the public sector to begin to define end goals to help drive concrete polycentric action.

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.[155] 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."[156] 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."[157] Consequently, regime complexes, as a form of bottom-up institution building, are becoming relatively more popular due to divergent interests. These divergent interests may have some benefits since negotiations for multilateral treaties could divert attention from more practical efforts to create flexible, loosely coupled regimes within

154 *Id.* at 49.
155 Keohane & Victor, *supra* note 145, at 7–8.
156 *Id.* at 9.
157 Oran R. Young, *Rights, Rules, and Resources in World Affairs*, *in* GLOBAL GOVERNANCE: DRAWING INSIGHTS FROM THE ENVIRONMENTAL EXPERIENCE 10 (Oran R. Young ed., 1997).

the IoE ecosystem.[158] An example of such a regime from Professor Joseph S. Nye, Jr. is included in Figure 5.

Figure 5: Professor Nye's Cyber Regime Complex Map[159]



But there are also the costs of regime complexes to consider. In particular, such networks are susceptible to institutional fragmentation and gridlock caused by overlapping authority that must still "meet standards of coherence, effectiveness, [and] . . . sustainability."[160] 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. To aid in this effort, scholars and policymakers should make use of the literature on modularity, which is "essential to the design of complex systems, considering that we have limited mental capabilities and can only process sub-segments of such systems at a time."[161] By identifying design rules for the architecture, interfaces, and integration protocols within the IoE, both governance

[158] Keohane & Victor, *supra* note 145, at 2.

[159] Joseph S. Nye, Jr., *The Regime Complex for Managing Global Cyber Activities* 8 (Global Comm'n on Internet Governance, Paper Series: No.1, May 2014), https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

[160] *Id.* at 2, 18–19, 25.

[161] JOSEF WALTL, IP MODULARITY IN SOFTWARE PRODUCTS AND SOFTWARE PLATFORM ECOSYSTEMS 20 (2013) (citing CARLISS YOUNG BALDWIN & KIM B. CLARK, DESIGN RULES: THE POWER OF MODULARITY 63 (2000)).

scholars and policymakers may be able to develop novel research designs and interventions to help promote cyber peace.

CONCLUSION

As has been argued, "there are no institutional panaceas for resolving complex social dilemmas."[162] Never has this arguably been truer than in the IoE context. 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 Internet of Everything. Cole aptly sums up the current situation as follows:

> Thanks primarily to Elinor Ostrom and her colleagues at the Ostrom Workshop in Political Theory and Policy Analysis, we have learned that common-property regimes are a viable third category of governance regimes for successfully managing natural common-pool resources over long periods of time. And we have gained some idea of the conditions under which common-property regimes seem more or less likely to succeed based on the 'design principles' Ostrom derived from her meta-analyses of hundreds of individual cases. Since then, despite increasing data collection and efforts to improve analytical methods, further progress toward understanding and diagnosing (let alone resolving) commons problems has been marginal (though hardly insignificant).[163]

Important questions remain about the utility of the Design Principles, the IAD, and GKC Frameworks to helping us govern the Internet of Everything. Still, 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 Internet of Everything demands novel methodologies, standards, and regimes. The Ostroms' legacy helps to shine a light on the path toward cyber peace.

---

[162] Cole, *supra* note 14, at 48.
[163] *Id*. at 64.