International Journal of Communication 14(2020), 2564–2588 1932–8036/20200005

The Emerging Institutionalization of Global Internet of Things Governance: A Network Approach

JAEWON R. CHOI
WENHONG CHEN
The University of Texas at Austin, USA

This study empirically investigates the institutionalization process of burgeoning global Internet of things (IoT) governance from a network perspective. Previous work privileges nation-states as the dominant agents shaping global ICT governance organizations at the expense of the growing presence of private sector actors. Meanwhile, despite its growing usefulness, past governance research tends to use network as a metaphor rather than a method. Addressing these critical gaps, we incorporate a network approach to institutions involved in IoT technical standard making to advance a networked understanding of global IoT governance. An analysis of comembership networks of four major IoT international organizations (i.e., Open Connectivity Foundation, oneM2M, Thread Group, and Institute of Electrical and Electronics Engineers) in 2017 and 2018 identified powerful private sector players shaping global IoT governance, the emerging trend of power consolidation at the core of the network, and growing industrial and regional diversity that would further complicate the formation and implementation of regulatory policy at both the global and national levels.

Keyword: Internet of things (IoT), ICT governance, comembership network, institutional theory

Technology adoption is affected by a wide range of social, economic, and political factors rather than being solely dependent on technological features (Douglas, 1987; Marvin, 1988). Rules and standards that shape the affordances and constraints of a certain technology have critical influence on how it is perceived and adopted by the general public. Thus, understanding the institutions and processes of global ICT governance that set rules and standards for specific ICTs has great scholarly and practical importance. This research centers on the emerging global governance of the Internet of things (IoT).

IoT has generated great attention in ICT and media industries. Enabling computing to virtually all objects around us, IoT is expected to drive innovations, transform competition dynamics, and advance the so-called industry 4.0 (Dutton, 2014). On the one hand, IoT technologies are on the continuum of fixed and mobile Internet development. It is hard to imagine that IoT governance would be a drastic departure from fixed and mobile Internet governance for which a handful of governments and corporations of the developed

---

Jaewon R. Choi: jwroycechoi@gmail.com
Wenhong Chen: wenhong.chen@austin.utexas.edu
Date submitted: 2019-07-02

world has set the rules and standards. On the other hand, IoT involves a vast expansion of the industrial scope beyond what has conventionally been defined as tech and telecom at a pivotal time as nations previously on the margin of global ICT governance (e.g., China, South Korea, India) gain prominence as innovation powerhouses and/or significant markets.

However, IoT research so far has been dominated by (1) technological or (2) business and information system studies centered on the maximization of technological and economic efficiency and effectiveness. Thus, most IoT research has focused on the business model or marketing of specific applications. Reflecting the general patterns in the larger ICT literatures, more attention on policy and ethical issues is urgently needed (Chen & Quan-Haase, 2018; Dutton, 2014). Although there is a small emerging literature on IoT policy issues, most studies stop at discussing policy challenges without empirical analysis. Limited attention has been paid to the formation of global IoT governance in spite of its strong practical and scholarly implications. Practically, it will provide insight for national and international IoT adoption and institutionalization. Scholarly, it will illustrate patterns and changes of power relations key to the political economy of digital infrastructure. Focusing on network patterns and dynamics of the institutionalization process, we address this important issue on the advent and growth of global IoT governance. More specifically, this study aims to identify important private sector actors in the network of global IoT standard setting.

In what follows, we first review work on ICT governance as well as the nascent literature on IoT governance to develop a theoretical framework that integrates institutional and network theory. This research, as far as we know, is one of the first efforts using network theories and analysis to provide a more systematic picture of global IoT governance. Results demonstrate the powerful players from private sectors in shaping global IoT governance, the emerging trend of power consolidation at the core of the global IoT governance network, and a growing diversity in terms of industrial and regional origin that would further complicate the formation and implementation of regulatory policy at both the global and national levels.

Literature Review

We start by defining ICT and IoT governance and previous discussions on IoT governance. Next, we provide a more detailed review of the ICT governance literature with particular focus on the multistakeholderism and articulate three types of actors in the global ICT governance structure that are likely to be active in the global IoT regime: national governments, international organizations, and transnational corporations. Building on these three actors, we argue for a networked understanding of global IoT governance.

ICT Governance and IoT Governance

The International Telecommunications Union (ITU; 2012) describes IoT as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" (p. 1). IoT involves smart connected objects collecting data using sensors (collection phase), communicating information through network (transmission phase), and generating useful information through data analysis to provide value-added services (processing, managing, and utilizing phase). This involves dissemination of myriad hardware devices with microsensors and complicated sets of software to engage in big data collection and analysis. As the next stage of global ICT infrastructure, the technological nature of IoT requires collaboration of corporations from diverse industries and geographic locations.

Governance is about the allocation of resources, roles, duties, and responsibilities among stakeholders. Governance, once mostly associated with government and states, has evolved as a more hybrid process involving multiple public and private stakeholders, often from multiple jurisdictions, coming together in networks (Bevir, 2011); the governance of the Internet and ICTs shares such characteristics. Global governance expands the process of "conducting the public's business—to the constellation of authoritative rules, institutions and practices by means of which any collectivity manages its affairs" to the global level (Ruggie, 2004, p. 504). It often involves a range of stakeholders with diverse interests that would establish governmental or nongovernmental organizations for multilateral negotiations. For instance, global Internet governance is established through stakeholders such as governments, the private sector, and civil society actors that jointly develop "shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet" (World Summit on the Information Society, 2005, p. 34). ICT governance has been a "rapidly changing ecology of technical artifacts, people, including users, and techniques that comprise what we view as the Internet and related ICTs" (Dutton, 2015, p. 17).

IoT is in its nascent but crucial stage in which hardware and software technologies are being developed, certified, and adopted as industry-specific applications. Therefore, this study primarily examines IoT governance in terms of technical standardization. It is currently a time when various institutions battle for global standards promoting their own agendas and interests. For complex ICT systems such as IoT, standards and protocols essentially function as the governing mechanism, and it is critical to examine how they are being institutionalized because global standards are never purely technical (DeNardis, 2009). IoT is one of the integral parts of the emerging "embedded infosphere," which calls for a reimagination of basic principles of traditional telecommunications and information policy (Taylor, 2017). In the context of such emerging technologies with uncertainties, the traditional regulatory approach with established "hard law" and legislation tends to be less effective and appropriate than "soft law" governance, which puts greater emphasis on a more informal model of regulations such as the coregulation of the private sector and the multistakeholder process in generating consensus on soft criteria (Hagemann, Huddleston, & Thierer, 2018). Therefore, studies on IoT governance should strive for more appropriate approaches that reflect informal governance. However, most previous IoT governance research has come from a legal perspective and has centered on issues such as the naming authority, the unique identification of IoT devices, privacy concerns, and accountability issues (Weber, 2011). There is still a lack of theory-driven empirical analysis. Our research provides an alternative perspective to incorporate complex relationships between and among major stakeholders involved in IoT governance formation.

Multistakeholderism in ICT Governance

A commonly surfacing theme in ICT governance research, especially in a global context, is *multistakeholderism*, which aims for more effective and meaningful participation from a broader range of stakeholders in ICT governance, ultimately creating potential new forms of "stakeholder democracy" (Bäckstrand, 2006). Despite the democratic ideal of multistakeholderism, the flexibility of loose definition of the concept has engendered varying interpretation regarding legitimacy, formation, and participants (Gasser, Budish, & West, 2015). A critique on multistakeholderism argues that in addition to its descriptive definitions involving a constellation of actors, it can be a fiction consisting of common imaginaries of global representation, democratization of the transnational sphere, and the possibility of improved outcomes (Hofmann, 2016). As important, there can be power imbalance between and among states, corporations, and civil society actors. However, the multistakeholder process has not only been established as a significant governance principle especially in the global context, but also is becoming an increasingly influential governance mechanism when it comes to emerging technologies such as IoT as it allows a wider range of stakeholders in addition to traditional governmental entities (Hagemann et al., 2018).

The majority of previous studies on global ICT governance has taken two approaches: (1) the history and activity of established international governance organizations (e.g., ITU, Internet Corporation for Assigned Names and Numbers, World Wide Web Consortium; Radu, Chenou, & Weber, 2013) or (2) a political economy critique on macro-level principles of global governance as well as pressing issues at hand (e.g., privacy, data security, etc.; Weber, 2010). Although both approaches mention the growing significance of nonstate actors, many studies highlight that nation-states still are prominent agents that shape global ICT governance organizations (Wallman, 2000). For instance, Whalley, Zhou, and An (2009) document how China as a nation-state successfully promoted its homegrown 3G standard as an international standard. Nation-states also play an integral role in the adoption and diffusion of ICT, especially in the context of developing countries (Choung, Hameed, & Ji, 2012; Liu & Gao, 2016). By contrast, the growing presence and influence of private sector actors have not been a primary concern in the existing literature. In this study, we put more focus on private sector-driven organizations and the relationships among prominent governance stakeholders of IoT rather than implications of the specific functioning of different IoT standards. Similar to ICT governance, we see emerging global IoT governance as an institutionalization process (Dacin, Goodstein, & Scott, 2002) shaped by interests, agency, and legitimacy of three types of interrelated stakeholders: nation-states, international organizations, and transnational corporations. Here, we follow the understanding that governance, especially in the global and IoT context, is the outcome of interactions among multiple actors (i.e., stakeholders) whose actions are enabled and constrained by institutions or, more broadly, the arrangements within and among institutions (Peters, 2011; Sørensen & Torfing, 2005). Therefore, in the following paragraphs, we describe the aforementioned three major stakeholders involved in the institutionalization process.

First, transnational telecommunication, Internet, and media corporations are pivotal figures in global Internet governance. Despite early utopian notions of the Internet highlighting its affordance of free speech, countercultural ethos, and libertarianism (Turner, 2006), the Internet has rapidly become one of the most profitable industries. Together, big telecommunication, tech, and media firms control information and content traveling through the Internet. Major tech firms such as Alphabet or Facebook have established themselves as platforms with tremendous power that shape the ways in which economic and public institutions operate (Cohen, 2017; van Dijck, Poell, & de Waal, 2018). Indeed, their oligopolistic if not monopolistic status in many national markets has led to a growing number of antitrust cases and calls for regulations (Ip, 2018).

Second, nation-states are perceived as one among several major “stakeholders” in global Internet governance (Mueller, 2010; Radu et al., 2013). Yet, Internet governance has challenged the dominance of the nation-state in global ICT governance because of the blurring of physical and temporal boundaries as well as distributed participation and control enabled by digital technologies. Domestically, deregulation and marketization have been the major policy approach regulating the telecom and media industries in most developed and many developing countries since the 1970s. Internationally, there has been an ideological shift from a traditional sovereignty-based approach in which nation-states shape the policy to multistakeholderism involving multiple stakeholders including but not limited to nation-states (DeNardis, 2009; Mueller, 2010).

Third, although the extent to which nation-states have declined remains an issues of debate (Straubhaar, 2007), the rise of international organizations, in the spirit of multistakeholderism, has been evident in several different forms as they become indispensable in multilateral negotiations on international economic, political, and security issues. International governmental organizations are the most common and publicly known, including regional ones such as the European Union or specialized ones such as the World Trade Organization. However, nongovernmental organizations, professional organizations, and industry alliances play important roles in advocating and pursuing group interests and legitimacy. Corporations strategically form and participate in industry alliances to capture or create value for growth and competency (O'Dwyer & Gilmore, 2018).

Global governance functions through getting multiple stakeholders together to set technical and industrial standards. Several international organizations, such as the World Wide Web Consortium and the Internet Corporation for Assigned Names and Numbers, have emerged to deal with myriad technical issues and standards related to Internet technology. Yet, the focus on the role of the nation-state leads to overlooking the significance of private sector power and how governance has transformed in a networked environment (DeNardis, 2009; Epstein, Katzenbach, & Musiani, 2016). There is a growing need to examine private platforms as active governance stakeholders (DeNardis & Hackl, 2015). The extensive marketization and privatization of ICT infrastructures have led to a power shift from nation-states to corporations. If nation-states were the prime figures of governance in traditional global politics, private corporations have become increasingly significant in global ICT governance dynamics especially after the advent of the Internet (DeNardis, 2009). However, the multistakeholderism in global Internet governance has its limitations as demonstrated in the debate between advocates of "cybersovereignty" reiterating Internet control by national governments and the proponents of the multistakeholder approach (Radu et al., 2013, p. 5). That is, it is important to show that some stakeholders are more prominent than others and how their positions may change over time.

ICT governance research also needs methodological innovation. Although there have been repeated calls for analyzing the complex networks of global media systems and conglomerates (Arsenault & Castells, 2008; Chen, 2018; Ognyanova & Monge, 2013; Radu et al., 2013; Weber, 2010), a large part of the Internet and IoT governance discussion has remained descriptive and primarily centered on historical trajectories and major events. Few studies have employed network analysis in investigating the global Internet or IoT governance structure. In what follows, we discuss how a network lens can help to illustrate the status and power dynamics of key stakeholders in the complicated landscape of global IoT governance.

A Networked Understanding of Global IoT Governance

Conceptualizing governance as a network enables the examination of the structural and relational aspects among the stakeholders as well as factors that affect their power distribution, interest construction, and interaction dynamics. In the context of global Internet governance, few studies have taken a network approach to map both online and offline networks around specific fields of Internet governance (Pavan, 2010; Pavan & Diani, 2008). Although researchers purport the network as an insightful analytic framework for investigating governance processes (Padovani & Pavan, 2012), there is still room for further empirical works especially as previous works have focused more on (1) semantic networks rather than interorganizational networks based on comembership and (2) standard setting of established rather than emerging technologies. Overall, despite the growing attention in using the network approach, it is still rarely used in governance research.

Various network attributes such as size, density, centrality, and position affect an actor's access to and mobilization of social capital for resources embedded in the network (Lin, 1999). Among the measures, one of the most widely used network concept is that of centrality (Borgatti, Mehra, Brass, & Labianca, 2009; Freeman, 1978; Marsden, 1990). Central players in a network are more able to obtain legitimacy and exert greater influence on issues important to members of the network. In particular, brokers who occupy structural holes between two otherwise disjunctive networks are in a unique position to generate financial or creative value (Burt, 2004). Brokerage and structural holes are relevant to global IoT governance based on the very nature of IoT at the intersection of device, software, and infrastructure that calls for collaborations and competitions among corporations from previously less connected or unconnected industries. A widely used measure of brokerage is *betweenness centrality*. By definition, betweenness centrality measures how often a given node falls along the shortest path between two other nodes (Borgatti, Everett, & Johnson, 2013). It implicates potential control or the capacity to enable or interrupt communication (Marsden, 1990). In other words, it reflects the extent to which an actor can play the role as gatekeeper, interpreter, or synthesizer in the network. In addition to betweenness centrality, *closeness centrality* refers to how close an actor is to all of the other actors in the network. High closeness centrality indicates an advantage of reaching out to and potentially influencing others in the network. This could be beneficial for achieving better compatibility and interoperability between different IoT standards and platforms. Thus,

RQ 1: Who are the important actors in the global IoT governance network in terms of betweenness and closeness centrality?

Furthermore, given the ongoing formation of IoT governance, a network lens allows us to observe how the network of global IoT changes and its implications over time. We have two types of changes in mind: first, the unfolding structural changes of the global IoT governance network such as changes in size, density, and interconnections between and among IoT governance institutions and stakeholders. The contours of such changes will shed light on whether the network is diversely expanding or centralizing, whether interconnections among certain institutions are strengthening or weakening, and whether different actors gain or loss power over time. Second, the national, regional, and industrial attributes of key actors allow us to see whether global IoT governance may differ from previous global ICT governance. Western developed countries have been the primary actors in previous global governance systems of the Internet and mobile. The United States has long been arguably the birthplace of the Internet and Europe as the home for ITU (DeNardis, 2009). Although we start to see corporations based on other regions emerge in the mobile space (e.g., Samsung from South Korea or Huawei from China), Western prominence persists in global Internet and mobile governance (J. Park, Kim, & Nam, 2015). Thus, a network analysis would illustrate the extent to which these dynamics may hold or vary in global IoT governance. Therefore, *RQ2a: What are the major changes in the global IoT governance network over time?*

RQ2b: In what way do the national, regional, and industrial characteristics of key actors of global IoT governance differ from those in previous global ICT governance?

Method and Data

IoT as a technology and an industry is still in an early stage. Accordingly, IoT research often suffers from a lack of reliable data, let alone network data. Filling this gap, we collected relational data from four major international organizations, including three private industry alliances (Open Connectivity Foundation [OCF], oneM2M, Thread Group) and a professional organization (Institute of Electrical and Electronics Engineers [IEEE]). These three alliances were selected because they have been identified as major institutions that shape IoT standardization activities (Meddeb, 2016; H. Park, Kim, Joo, & Song, 2016) and their standard solutions connect multiple layers of IoT service development, and IEEE P2413, a working group under IEEE, is a major professional institution actively pursuing IoT-related standard initiatives (O'Donnell, 2016; see Table 1). The importance of these organizations supports our argument of paying greater attention to private industry alliances of corporations and nongovernmental international organizations as active agents shaping global IT governance, whereas previous studies have tended to privilege nation-states and intergovernmental organizations in global ICT governance (DeNardis & Hackl, 2015). Indeed, there has been a relative lack of national government engagement in global IoT governance (National Telecommunications and Information Administration, 2017).

Table 1. Internet of Things Organizations, Standards, and Characteristics.

Name	Standard	Type	Year	Headquarters	Note
OCF (Open Connectivity Foundation)	IoTivity, AllJoyn	Industry alliance	2016	United States	• Open Interconnect Consortium (OIC) + AllSeen consolidation • OIC: Led by Samsung • AllSeen: Led by LG Electronics
Thread Group	Thread Framework	Industry alliance	2014	United States	• Alphabet's initiative related to Google Nest
oneM2M	oneM2M	Hybrid alliance	2012	N/A	• Eight regional standard development organizations
Institute of Electrical and Electronics Engineers (IEEE) P2413	IEEE P2413	International organization	2015	United States	

OCF, formerly Open Interconnect Consortium, was founded in 2014 by Intel, Broadcom, and Samsung Electronics. Broadcom left the consortium early, and the Open Interconnect Consortium re-established itself as OCF in 2016, adding new members including major corporations such as Microsoft, Qualcomm, and Electrolux. Merging with the Qualcomm-led IoT alliance AllSeen Alliance in 2016, OCF is one of if not the most visible market-led industry alliance pushing the IoT standards agenda shaping global IoT governance.

Thread Group was also founded in 2014 as a working group specializing in IoT "smart" home automation systems. It was formed around Google's subsidiary Nest Labs. Despite its relatively narrow focus, it consists of several influential industry players such as Samsung, Arm Holdings, Qualcomm, and Silicon Labs.

oneM2M was established in 2012. Its composition is quite different from other private industry alliances, with both private corporations and eight standards development organizations from major nations and five global industry fora, consortia, or standards bodies.[1]

IEEE is an international professional association of engineers, scientists, and developers in computer science, electronic engineering, and other IT fields. The association consists of both individual and corporate members. The IEEE Standards Association has been an active player in standard making. In this study, we focused on IEEE P2413, IEEE's working group pursuing standards for the architectural framework for IoT.

Networks over time could inform about the specific mechanisms that construct the governance structure (De Reuver & Bouwman, 2012). We collected and compiled two data sets at two time points: April 2017 (T1) and July 2018 (T2). The resulting networks were two two-mode cross-membership networks of 286 (T1) and 250 (T2) actors in four alliances/organizations. In each data set, we inferred the existence of a relationship between any two actors by looking at their concurrence in the membership list of the four organizations. The three private industry alliances have strict membership levels based on the amount of membership fee, which determines the extent to which a member can participate in and benefit from the alliance's pooled resources such as intellectual properties. For instance, the OCF has more than 400 members in five levels. Membership in the top two levels requires substantial annual fees, but members have voting rights for decision making; however, most members are basic members who pay no annual fee. In general, these lower level members are restricted from accessing intellectual properties and actively participating in work groups or meetings, and are allowed only limited access (e.g., read-only) to documents and other alliance resources.

[1] Eight regional ICT standards development organizations include Association of Radio Industries and Businesses (Japan), Alliance for Telecommunications Industry Solutions (United States), China Communications Standards Association (CCSA, China), European Telecommunications Standards Institute (Europe), Telecommunications Industry Association (TIA, United States), Telecommunications Standards Development Society, India (India), Telecommunications Technology Association (TTA, South Korea), and Telecommunication Technology Committee (TTC, Japan); five industry consortia consist of Broadband Forum, Comité Européen de Normalisation (European Committee for Standardization), European Committee for Electrotechnical Standardization, Global Platform, and Open Mobile Alliance (OMA).

To maintain a reasonable sample size of participants with considerable stakes in the alliances, only those members in the top two membership levels in the three alliances were included. IEEE P2413 has no indication of levels of participation or access to resources. Therefore, we included all IEEE P2413 members. We created two projections in the organization level and actor level to ensure a more accurate representation of the different levels of the "two-mode" network (Conaldi, Lomi, & Tonellato, 2012). In addition to general descriptive measures on node degree and density, we focused on betweenness centrality and closeness centrality to identify important actors (RQ1) and changes (RQ2). The analysis was done using the R igraph package for network analysis (Csardi & Nepusz, 2006). Figure 1 and Figure 2 visualize the global IoT governance networks at T1 and T2, respectively.

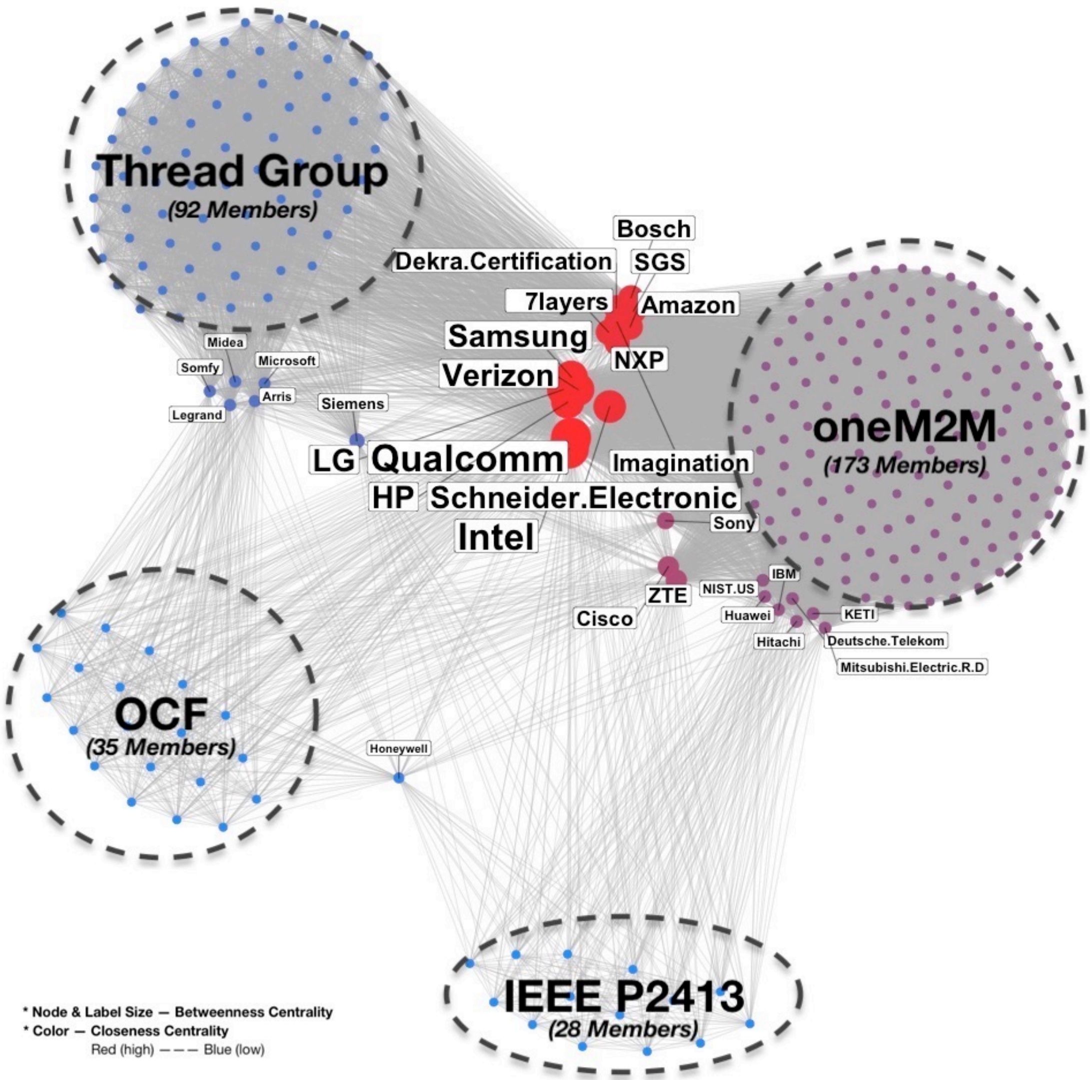

Figure 1. Global Internet of things governance network (April 2017). OCF = Open Connectivity Foundation; IEEE = Institute of Electrical and Electronics Engineers.

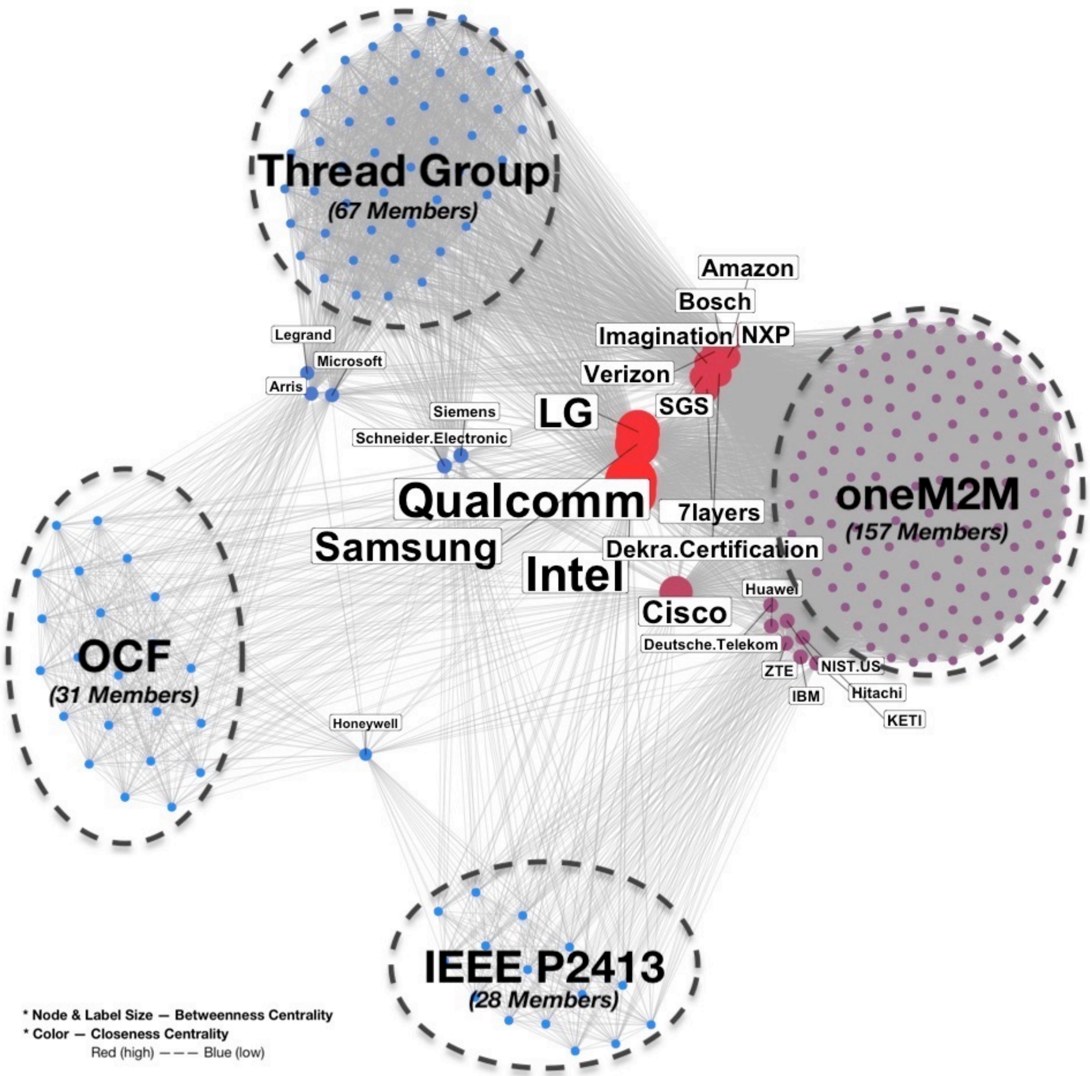

Figure 2. Global Internet of things governance network (July 2018). OCF = Open Connectivity Foundation; IEEE = Institute of Electrical and Electronics Engineers.

Results: Actors (RQ1) and Changes (RQ2) in the Global IoT Governance Network

Actor-Level and Organizational-Level Centrality

The centrality measure analysis showed actors that were more central than others. Table 2 summarizes the degree, betweenness centrality, closeness centrality, and basic attributes of the actors at T1 and T2. Overall, at T1 in 2017, 31 actors had a greater than average betweenness centrality (M = 74.03). At T2 in 2018, 26 actors had a greater than average betweenness centrality (M = 64.41). This could imply a consolidation of power in the network of global IoT governance as fewer players possessed the broker capacity to connect different actors in key IoT organizations. Although the rankings fluctuated from T1 to T2, players with substantial brokerage roles remained similar.

Table 2. Internet of Things Governance Network Centrality Measures (Ranked by Betweenness Centrality).

	Time 1 (Density = .4858)						Time 2 (Density = .4870)					
Rank	Node	Headquarters	Main industry	Degree (*M*=138)	Closeness (*M*=.00233)	Betweenness (*M*=74.03)	Node	Headquarters	Main industry	Degree (*M*=121)	Closeness (*M*=.00269)	Betweenness (*M*=64.41)
1	Intel	United States	Hardware	285	.00311	1710.14	Intel	United States	Hardware	249	.00361	1806.28
2	Qualcomm	United States	Hardware	285	.00311	1710.14	Qualcomm	United States	Hardware	249	.00361	1806.28
3	LG Electronics	South Korea	Hardware	271	.00308	1320.88	LG Electronics	South Korea	Hardware	234	.00355	1455.29
4	Samsung	South Korea	Hardware	271	.00308	1320.88	Samsung	South Korea	Hardware	234	.00355	1455.29
5	Hewlett-Packard	United States	Hardware	271	.00308	1320.88	Cisco	United States	Hardware	199	.00319	1025.41
6	Verizon	United States	Telecom	271	.00308	1320.88	Verizon	United States	Telecom	211	.00336	666.86
7	Schneider Electric	France	Hardware	265	.00303	1299.04	NXP	Netherlands	Hardware	211	.00336	666.86
8	NXP	Netherlands	Hardware	250	.00300	903.94	7layers	Germany	Certification	211	.00336	666.86
9	7layers	Germany	Certification	250	.00300	903.94	Dekra Certification	Netherlands	Certification	211	.00336	666.86
10	Dekra Certification	Netherlands	Certification	250	.00300	903.94	Imagination	England	Hardware	211	.00336	666.86
11	Imagination	England	Hardware	250	.00300	903.94	Amazon	United States	E-commerce	211	.00336	666.86

	Time 1 (Density = .4858)						Time 2 (Density = .4870)					
Rank	Node	Headquarters	Main industry	Degree (*M*=138)	Closeness (*M*=.00233)	Betweenness (*M*=74.03)	Node	Headquarters	Main industry	Degree (*M*=121)	Closeness (*M*=.00269)	Betweenness (*M*=64.41)
12	Amazon	United States	E-commerce	250	.00300	903.94	Bosch	Germany	Hardware	211	.00336	666.86
13	Bosch	Germany	Hardware	250	.00300	903.94	SGS	Switzerland	Certification	211	.00336	666.86
14	SGS	Switzerland	Certification	250	.00300	903.94	Schneider Electric	France	Hardware	90	.00243	257.03
15	Cisco	United States	Hardware	213	.00265	679.27	Siemens	Germany	Hardware	90	.00243	257.03
16	ZTE	China	Hardware	213	.00265	679.27	ZTE	China	Hardware	174	.00300	251.85
17	Sony	Japan	Hardware	198	.00263	458.36	Deutsche Telekom	Germany	Telecom	174	.00300	251.85
18	Siemens	Germany	Hardware	115	.00218	346.48	Hitachi	Japan	Hardware	174	.00300	251.85
19	Deutsche Telekom	Germany	Telecom	188	.00254	211.13	Huawei	China	Hardware	174	.00300	251.85
20	Hitachi	Japan	Hardware	188	.00254	211.13	IBM	United States	Hardware	174	.00300	251.85
21	Huawei	China	Hardware	188	.00254	211.13	Korea Electronics Technology Institute	South Korea	Research Institute	174	.00300	251.85

	Time 1 (Density = .4858)						Time 2 (Density = .4870)					
Rank	Node	Headquarters	Main industry	Degree (*M*=138)	Closeness (*M*=.00233)	Betweenness (*M*=74.03)	Node	Headquarters	Main industry	Degree (*M*=121)	Closeness (*M*=.00269)	Betweenness (*M*=64.41)
22	IBM	United States	Hardware	188	.00254	211.13	National Institute of Standards and Technology	United States	Research institute	174	.00300	251.85
23	Korea Electronics Technology Institute	South Korea	Research institute	188	.00254	211.13	Microsoft	United States	Software	90	.00242	219.26
24	Mitsubishi Electric	Japan	Hardware	188	.00254	211.13	Arris	United States	Hardware	90	.00242	219.26
25	National Institute of Standards and Technology	United States	Research institute	188	.00254	211.13	Legrand	France	Hardware	90	.00242	219.26
26	Microsoft	United States	Software	115	.00215	176.85	Honeywell	United States	Hardware	54	.00224	156.53
27	Arris	United States	Hardware	115	.00215	176.85						
28	Legrand	France	Hardware	115	.00215	176.85						
29	Midea	China	Hardware	115	.00215	176.85						
30	Somfy	France	Hardware	115	.00215	176.85						
31	Honeywell	United States	Hardware	57	.00193	109.73						

Indicated by betweenness centrality (*BC*), large international corporations, namely Intel, Qualcomm, LG Electronics, and Samsung, were the top four ranked brokers at both time points. Hewlett-Packard, Schneider Electric, and 7layers dropped out from the top-10 list of brokers from T1 to T2. One noticeable actor was Honeywell, a U.S.-based electronic appliance and hardware manufacturer, a significant broker at both T1 (*BC* = 109.73) and T2 (*BC* = 156.53), even though it had only a low number of ties. That is, Honeywell managed to maintain connections with diverse parts of the global IoT governance network with relatively few relationships. In terms of closeness centrality (*CC*), the top four players resembled those of betweenness centrality at both T1 and T2: Intel, Qualcomm, LG Electronics, and Samsung. Hewlett-Packard and Verizon were the top four at T1; however, Hewlett-Packard's significance dropped at T2, ranking Verizon as fifth. Interestingly, Honeywell, a key broker, had considerably low closeness centrality, ranked 252nd and 213th, respectively, at T1 and T2. That is, although the company was well situated as a broker, Honeywell was not able to quickly reach out to or access information or resources from a larger number of peers in the global IoT governance network.

Basic descriptive network analysis at the organization level showed that oneM2M was the largest institution with 173 members in 2017 and 157 in 2018, followed by Thread Group with 92 members in 2017 and 67 in 2018. Furthermore, the four organizations maintained close ties at both time points. Most interesting, IEEE was the top broker among the four organizations at T1 in 2017 (normalized betweenness = 0.33), but this role was taken over by OCF at T2 in 2018 (normalized betweenness = 0.5).

Changes: Size, Density, and Comembership

The size of the global IoT governance network decreased while density (*D*) increased (D_{T1} = .4858 to D_{T2} = .4870) from T1 to T2. The shrinking size over one year was more noticeable in the private alliances than in the professional organizations. The decline of network size occurred in the periphery rather than at the core. Over a year, from 2017 and 2018, 75 actors disappeared from the global IoT governance network and 39 new actors joined. Several notable conglomerates such as Philips or Sprint left, when such companies as John Deere (a major agricultural and heavy equipment manufacturer) or Hyundai Motor Group became new members. Although it is unclear whether the decrease was a trend, it certainly demonstrates the volatility of an emerging industry with disruptively innovative product and service but uncertain return, especially for those firms whose core business was not ICT business.

The numbers of shared members among the organizations decreased from 2017 to 2018, corresponding with the decline of overall network size. In particular, the number of shared members between OCF and Thread Group dropped from 11 to seven, followed by the number of shared members between OCF and oneM2M from nine to five. Meanwhile, all three private industry alliances maintained similar comembers with IEEE. That is, the comembership among the three private industry alliances was shifting, but all of them maintained a relatively stable relationship with the professional community.

National, Regional, and Industrial Attributes

Here, we further examined regional and national origins of the key actors of the global IoT governance network at T1 and T2. By region, we used broader conceptualization at the continent level. The analysis showed that actors with higher than average centrality values mainly came from North America, Europe, and Asia.[2] In 2017, the three regions were distributed relatively evenly in the global IoT governance network, whereas the United States and Europe each had 11 central players, and Asia had nine. In 2018, the United States and Europe each had 10 key players, and Asia had six.

At the national level, more than one third of the key actors originated from the United States at both time points, followed by German firms (12.9% of the key actors with a high betweenness centrality in 2017 and 15.4% in 2018). South Korean, Japanese, Chinese, and French firms accounted for about 9.7% among the key players in 2017. This changed over time as the share of South Korean actors increased to 11.5%, and Chinese (7.7%), French (7.7%), and Japanese (3.8%) players experienced slight decreases. The number of key actors from the Netherlands (n = 2), England (n = 1), and Switzerland (n = 1) remained the same.

In terms of industrial background, we found greater industrial diversity when compared with previous global governance of ICT. A number of corporations that were not directly involved in traditional ICT industries surfaced as brokers. For instance, the industrial backgrounds of Schneider Electric, Bosch GmbH, Hitachi, Siemens, and Mitsubishi ranged from home appliances and electronics to energy management, demonstrating the growing and contesting interest in IoT from distinct industry sectors. Furthermore, the prominence of corporations such as 7layers and Dekra Certification was noteworthy. The 7layers group is an affiliate of the Bureau Veritas Group, which provides services of testing, inspection, and certification of various wireless technologies. The central position of certification firms in the network reflects the industry's push for building credibility and legitimacy through standardization.

Conclusion, Contribution, and Discussion

This study empirically investigates the pattern and process of institutionalization of global IoT governance in its nascent stage from a network perspective. It makes both theoretical and practical contribution. Previous work seems to privilege nation-states as the dominant agents that shape global ICT governance organizations at the expense of the growing presence and influence of private sector actors. Although the efforts of setting ICT standards have been highly market-driven, scholarly discussions of private sector endeavors in global governance remain rare. We are interested in the role of nongovernmental organizations such as private sector alliances, which has been downplayed if not overlooked in the existing literature. Meanwhile, although the network has emerged as a useful way of understanding governance structure (Slaughter, 2004), past work has tended to use it as a metaphor rather than a method. This study sees the institutionalization of global IoT governance as an emerging and evolving network. This contributes to the literature by providing a viable analytical framework with empirical evidence that could be useful for examining multistakeholderism-based global ICT governance and beyond.

Our study incorporates network theory and methods for an empirical investigation of nongovernmental organizations such as industry alliances and professional organizations in global IoT

---

[2] In total, nine countries represented these three regions: South Korea, Japan, China (Asia), England, the Netherlands, Switzerland, Germany, France (Europe), and the United States.

governance. Our exploratory analysis of the comembership network of four key international organizations involved in the IoT governance yields important insights. We identified central actors in the global IoT governance network in terms of betweenness and closeness centrality (RQ1). Moreover, data collected in two time points allowed us to observe changes of the global IoT governance network in the period of a year as well as when compared with previous global ICT governance. Below, we summarize our major findings on the key players (RQ1) and network changes (RQ2).

First, traditional ICT conglomerates such as Intel, Qualcomm, LG Electronics, Samsung, and Verizon were the most important brokers, demonstrating their roles in initiating the formation of key industry alliances. For instance, Intel and Samsung were the initiators of the Open Internet Consortium, and LG Electronics and Qualcomm were leading the AllSeen alliance, which later consolidated into OCF. Closeness centrality analysis surfaced similar players that also had high ranking of betweenness centrality such as Intel, Qualcomm, LG Electronics, Samsung, and Verizon. That is, brokers in the global IoT governance network command strategic positions to quickly reach out to the rest of the network as well as to facilitate the flow of information and influence. One interesting exception was Honeywell as a relatively "isolated" broker that scored high in betweenness but low in closeness centrality.[3] Regarding the power dynamics, these brokers are more likely to exert "bargaining power" connecting otherwise less connected actors to broader network (Padovani & Pavan, 2011).

Second, a comparative analysis over a one-year period from 2017 to 2018 shows that the size of the network decreased while the density increased. Considering that the central players remained central from T1 to T2, change occurred more in the periphery than at the center. That is, the network of global IoT governance became smaller and denser, with fewer powerful actors controlling information flow and agenda setting. Taking into account the growing concentration in the media and telecommunication industries—both highly relevant to the burgeoning IoT industry—in the last several years, our result suggests a consolidation of key players at a fairly early stage of global IoT governance.

Third, we identified some evidence of greater industrial and regional diversity when compared with the global governance of previous ICTs such as the Internet and mobile. A number of corporations, prominently from electronics industry as well as the testing, inspection, and certification service, which previously were not directly involved or commanding a highly influential position in the Internet industry, have a brokering position in the IoT governance network. Our network analysis suggests a growing regional diversity in the formation of global IoT governance compared with the primarily U.S.-centered development of global Internet governance (Turner, 2006). Regionally, many Asian and European players have acquired pivotal positions within the network despite the persisting prominence of American conglomerates.

To recap, we underscore three major findings. First is the significance of private organizations in shaping the agenda and discourse of IoT global governance as they are interconnected via industry alliances

---

[3] Honeywell has been actively moving into the IoT space, especially the industrial Internet of things solutions serving business clients to automate their business processes. In 2016, Honeywell established a separate IoT-based unit Digital Transformation as part of Honeywell Process Solutions and launched the Uniformance Suite as the corporation's analytics platform for digital intelligence.

as well as through the authoritative international standards-making organizations such as IEEE. Second is the emerging trend of power consolidation at the core of the global IoT governance network at such an early stage of IoT development within a short time period. A handful of prominent players seems to have consolidated power at the center of the network as brokers and influencers. Our results are alarming as the global IoT governance network and the IoT industry seem to follow rather than challenge the path of media and telecommunication industries that have become a highly concentrated oligopoly under the regulatory regime emphasizing competition and market-driven innovation (Crawford, 2013; Hesmondhalgh, 2015). The third finding is that, consolidation of power aside, there is a growing diversity in terms of industrial and regional origin that would further complicate the formation and implementation of regulatory policy at both the global and national levels. If industrial diversity is expected given the convergent nature of IoT, regional diversity in early global IoT governance comes from European and Asian actors as brokers, in contrast to the predominantly U.S.-centered early development of the Internet.

Our findings have strong policy implications. First, policymakers should take the influence of private sectors in global ICT governance into greater account. The sign of consolidation over such a short time calls for policymakers' attention to potential industry concentration. Second, the increasing diversity in industry and regional origins in IoT governance is likely to make the formation of regulatory work more complex, which calls for new sets of legal frameworks (Weber, 2016). For corporations, it is critical to be alert to who is shaping the IoT discussion, including collaborators and competitors from both within and beyond their own industry. As it remains uncertain whether one single IoT standard will become dominant or multiple standards and protocols would coexist, it is critical for firms to develop product and service strategies that allow compatibility and interoperability.

The global IoT governance network we examined here as of July 2018 was heavy on technical standards for IoT devices, with most significant actors from electrical or telecommunications hardware manufacturers. The low profile of prominent tech firms such as Apple, Alphabet/Google, Facebook, or Amazon in the global IoT governance network as of Summer 2018 deserves discussion. Alphabet/Google, as the parent company of Nest, is closely related to the Thread Group. Amazon was ranked 12th and 11th in terms of betweenness centrality. However, Apple and Facebook are yet to surface in the network. First, the de facto IoT service standards are expected to emerge after the establishment of technical standards. This layer is an integral aspect in providing IoT services in everyday life such as data gathering, data processing, and representation involving complex software structure such as artificial intelligence. As IoT moves fast to a broader commercial release phase, the competition of de facto service standards may quickly cement the dominance of tech giants. Second, these tech giants are highly relevant as they control digital platforms that function as an integral part of digital infrastructure (van Dijck et al., 2018). Indeed, they have started competing in the consumer IoT industry by launching home automation devices and software, aiming to be the hub that allows users to control various IoT devices.[4] As the interface among users, devices,

---

[4] Following Amazon's lead with Amazon Echo and integrated digital artificial intelligence system Amazon Alexa, Apple and Google joined the competition with Apple HomePod with Siri and Google Home with its own artificial intelligence assistant system. Facebook, the global social media giant, has been slowly moving into similar business after acquiring a mobile app development platform Parse, a mobile operating system with native software development kit for creating apps for IoT devices, in 2013. With Facebook Portal, a

and algorithms, these platforms are likely to play a more crucial role in shaping public perception and social norms around IoT than technological standards.

This research has several limitations. First, our data are not an exhaustive description of the IoT governance that include all stakeholders. We focused on comembership in key global IoT organizations. Yet, there are other forms of network relationships such as economic exchange or political alliance among the players that were not captured in this study. Last, we note that the network measures examined in this study might not directly represent network actors' actual power or influence in IoT governance. This is because there are other forms of network ties in different levels (e.g., semantic network) that were not examined in this study (Padovani & Pavan, 2011). Nonetheless, we are convinced that this study is one of the first to theorize and empirically analyze the global governance initiatives concerning IoT governance as network.

This study can inform and inspire future research along the following lines. First, a more comprehensive data set with greater scope and depth would provide more insights. For instance, additional actor attributes would enable attribute-based network analysis and examining multiple types of network ties would provide a better understanding of the IoT governance network. Furthermore, a longer window of observation would allow researchers to see network changes for a longer period of time and see whether the dynamics in the alliance structure identified in this study gains or loses momentum. Finally, it would be highly interesting to build on our findings by empirically comparing the network structure of previous global ICT governance and IoT governance. Such work will highlight not only the similarities and distinctions of global governance networks as technologies advance, but also the power shift between and among key stakeholders. Last but not least, we should note the absence of activists and civil society in the IoT governance network we observed. Lack of their presence has been addressed as a major drawback and limitation of the current implementation of the multistakeholderism ideal. However, the social, cultural stake of IoT is as big, if not greater than, as that of the Internet and mobile. Therefore, we call for greater attention from and to the civil society actors and their activities that may shape global IoT governance.

References

Arsenault, A. H., & Castells, M. (2008). The structure and dynamics of global multi-media business networks. *International Journal of Communication*, *2*, 707–748.

Bäckstrand, K. (2006). Democratizing global environmental governance? Stakeholder democracy after the World Summit on Sustainable Development. *European Journal of International Relations*, *12*(4), 467–498. https://doi.org/10.1177/1354066106069321

Bevir, M. (2011). Governance as theory, practice, and dilemma. In M. Bevir (Ed.), *The SAGE handbook of governance* (pp. 1–16). London, UK: SAGE Publications.

video-calling device with similar functions as Echo and HomePod, the social media giant is on its way to enter the IoT business.

Borgatti, S. P., Everett, M. G., & Johnson, J. C. (2013). *Analyzing social networks*. London, UK: SAGE Publications.

Borgatti, S. P., Mehra, A., Brass, D. J., & Labianca, G. (2009). Network analysis in the social sciences. *Science*, *323*(5916), 892–895. https://doi.org/10.1126/science.1165821

Burt, R. S. (2004). Structural holes and good ideas. *American Journal of Sociology*, *110*(2), 349–399. https://doi.org/10.1086/421787

Chen, W. (2018). Abandoned not: Media sociology as a networked transfield. *Information, Communication & Society*, *21*(5), 647–660. https://doi.org/10.1080/1369118X.2018.1428658

Chen, W., & Quan-Haase, A. (2018). Big data ethics and politics: Toward new understandings. *Social Science Computer Review*, *38*, 1–7. https://doi.org/10.1177/0894439318810734

Choung, J. Y., Hameed, T., & Ji, I. (2012). Catch-up in ICT standards: Policy, implementation and standards-setting in South Korea. *Technological Forecasting and Social Change*, *79*(4), 771–788. https://doi.org/10.1016/j.techfore.2011.10.007

Cohen, J. E. (2017). Law for the platform economy. *U.C. Davis Law Review*, *51*(133), 133–204. Retrieved from https://heinonline.org/HOL/Page?handle=hein.journals/davlr51&id=139&div=8&collection=journals

Conaldi, G., Lomi, A., & Tonellato, M. (2012). Dynamic models of affiliation and the network structure of problem solving in an open source software project. *Organizational Research Methods*, *15*(3), 385–412. https://doi.org/10.1177/1094428111430541

Crawford, S. (2013). *Captive audience: The telecom industry and monopoly power in the new gilded age*. New Haven, CT: Yale University Press.

Csardi, G., & Nepusz, T. (2006). The igraph software package for complex network research. *InterJournal*, *Complex Systems*, 1695.

Dacin, M. T., Goodstein, J., & Scott, W. R. (2002). Institutional theory and institutional change: Introduction to the special research forum. *Academy of Management Journal*, *45*(1), 43–56.

DeNardis, L. (2009). *Protocol politics: The globalization of Internet governance*. Cambridge, MA: MIT Press.

DeNardis, L., & Hackl, A. M. (2015). Internet governance by social media platforms. *Telecommunications Policy*, *39*(9), 761–770. https://doi.org/10.1016/j.telpol.2015.04.003

De Reuver, M., & Bouwman, H. (2012). Governance mechanisms for mobile service innovation in value networks. *Journal of Business Research*, *65*(3), 347–354. https://doi.org/10.1016/j.jbusres.2011.04.016

Dijck, J. van, Poell, T., & de Waal, M. (2018). *The platform society: Public values in a connective world*. New York, NY: Oxford University Press.

Douglas, S. J. (1987). *Inventing American broadcasting, 1899–1922*. Baltimore, MD: Johns Hopkins University Press.

Dutton, W. H. (2014). Putting things to work: Social and policy challenges for the Internet of things. *Info*, *16*(3), 1–21. https://doi.org/10.1108/info-09-2013-0047

Dutton, W. H. (2015, June 7). *Multistakeholder Internet governance?* (Quello Center Working Paper No. 2615596). Quello Center, Michigan State University, East Lansing. https://doi.org/10.2139/ssrn.2615596

Epstein, D., Katzenbach, C., & Musiani, F. (2016). Doing Internet governance: Practices, controversies, infrastructures, and institutions. *Internet Policy Review*, *5*(3), 1–14. https://doi.org/10.14763/2016.3.435

Freeman, L. C. (1978). Centrality in social networks conceptual clarification. *Social Networks*, *79*(1), 215–239.

Gasser, U., Budish, R., & West, S. M. (2015). *Multistakeholder as governance groups: Observations from case studies* (Berkman Center Research Publication No. 2015-1). Berkman Klein Center for Internet & Society, Harvard University. https://doi.org/10.2139/ssrn.2549270

Hagemann, R., Huddleston, J., & Thierer, A. D. (2018). Soft law for hard problems: The governance of emerging technologies in an uncertain future. *Colorado Technology Law Journal*, *17*(1), 37–130.

Hesmondhalgh, D. (2015). Marketisation in telecommunications and broadcasting. In D. Hesmondhalgh, *The cultural industries* (3rd ed., pp. 121–153). London, UK: SAGE Publications.

Hofmann, J. (2016). Multi-stakeholderism in Internet governance: Putting a fiction into practice. *Journal of Cyber Policy*, *1*(1), 29–49. https://doi.org/10.1080/23738871.2016.1158303

Ip, G. (2018, January 16). The antitrust case against Facebook, Google, and Amazon. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/the-antitrust-case-against-facebook-google-amazon-and-apple-1516121561

International Telecommunications Union. (2012). *Overview of the Internet of things* (Recommendation ITU-T Y.2060). Geneva, Switzerland: Author. Retrieved from https://www.itu.int/rec/T-REC-Y.2060-201206-I

Lin, N. (1999). Social networks and status attainment. *Annual Review of Sociology*, *25*, 467–487.

Liu, G., & Gao, P. (2016). Government intervention in technology innovation system in the catching-up context: Case of TD-LTE technology innovation in China. In *Proceedings of the Ninth International Conference on Standardization and Innovation in Information Technology* (pp. 1–9). Piscataway, NJ: Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/SIIT.2015.7535602

Marsden, P. V. (1990). Network data and measurement. *Annual Review of Sociology*, *16*, 435–463.

Marvin, C. (1988). *When old technologies were new: Thinking about electric communication in the late nineteenth century*. New York, NY: Oxford University Press.

Meddeb, A. (2016). Internet of things standards: Who stands out from the crowd? *IEEE Communications Magazine*, *54*(7), 40–47. https://doi.org/10.1109/MCOM.2016.7514162

Mueller, M. L. (2010). *Networks and states: The global politics of Internet governance*. Cambridge, MA: MIT Press. Retrieved from http://www.jstor.org/stable/j.ctt5hhcz0

National Telecommunications and Information Administration. (2017). *Fostering the advancement of the Internet of things*. Retrieved from https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

O'Donnell, L. (2016, September 19). *10 IoT consortiums, alliances solution providers should have on their radar*. Retrieved from https://www.crn.com/slide-shows/internet-of-things/300082087/10-iot-consortiums-alliances-solution-providers-should-have-on-their-radar.htm/1

O'Dwyer, M., & Gilmore, A. (2018, February). Value and alliance capability and the formation of strategic alliances in SMEs: The impact of customer orientation and resource optimisation. *Journal of Business Research*, *87*, 58–68. https://doi.org/10.1016/j.jbusres.2018.02.020

Ognyanova, K., & Monge, P. (2013). A multitheoretical, multilevel, multidimensional network model of the media system: Production, content, and audiences. *Communication Yearbook*, *37*, 66–93. https://doi.org/10.1080/23808985.2013.11679146

Padovani, C., & Pavan, E. (2011). Actors and interactions in global communication governance: The heuristic potential of a network approach. In R. Mansell & M. Raboy (Eds.), *The handbook of global media and communication policy* (pp. 543–563). Oxford, UK: Wiley-Blackwell.

Padovani, C., & Pavan, E. (2012). International norms and socio-technical systems: Connecting institutional and technological infrastructures in governance processes. In *IFIP International Conference on Human Choice and Computers* (pp. 56–65). Berlin, Germany: Springer.

Park, H., Kim, H., Joo, H., & Song, J. S. (2016). Recent advancements in the Internet-of-things related standards: A oneM2M perspective. *ICT Express*, *2*(3), 126–129. https://doi.org/10.1016/j.icte.2016.08.009

Park, J., Kim, S., & Nam, C. (2015). Why has a Korean telecommunications technology failed? A case study on WiBro. *Telematics and Informatics*, *32*(4), 603–612. https://doi.org/10.1016/j.tele.2015.01.002

Pavan, E. (2010). Semantic and social networks on Internet governance: Inquiring the cognitive-side of global governance processes. In *Proceedings of the 40th European Consortium of Political Research* (pp. 1–20). Munster, Germany.

Pavan, E., & Diani, M. (2008, December). *Structuring online and offline discursive spaces on Internet governance: Insights from a network approach to map an emergent field*. Paper presented at GigaNet: Global Internet Governance Academic Network, Annual Symposium 2008. Hyderabad, India. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2798965

Peters, B. G. (2011). Institutional theory. In M. Bevir (Ed.), *The SAGE handbook of governance* (pp. 78–90). London, UK: SAGE Publications.

Radu, R., Chenou, J.-M., & Weber, R. H. (Eds.). (2013). *The evolution of global Internet governance: Principles and policies in the making*. London, UK: Springer.

Ruggie, J. G. (2004). Reconstituting the global public domain: Issues, actors, and practices. *European Journal of International Relations*, *10*(4), 499–531. https://doi.org/10.1177/1354066104047847

Slaughter, A.-M. (2004). *A new world order*. Princeton, NJ: Princeton University Press.

Sørensen, E., & Torfing, J. (2005). The democratic anchorage of governance networks. *Scandinavian Political Studies*, *28*(3), 195–218. https://doi.org/10.1111/j.1467-9477.2005.00129.x

Straubhaar, J. D. (2007). *World television: From global to local*. Los Angeles, CA: SAGE Publications.

Taylor, R. D. (2017). The next stage of U.S. communications policy: The emerging embedded infosphere. *Telecommunications Policy*, *41*(10), 1039–1055. https://doi.org/10.1016/j.telpol.2016.11.007

Turner, F. (2006). *From counterculture to cyberculture: Stewart Brand, the Whole Earth network, and the rise of digital utopianism*. Chicago, IL: University of Chicago Press.

Wallman, K. M. H. (2000). The role of government in telecommunications standard-setting. *CommLaw Conspectus: Journal of Communications Law and Policy*, *8*(2), 235–252.

Weber, R. H. (2010). Governance of the Internet of things. In H. Chaouchi (Ed.), *Internet of things: Connecting objects to the Web* (pp. 69–100). London, UK: International Society for Technology in Education. https://doi.org/10.1007/978-3-642-11710-7_4

Weber, R. H. (2011). Accountability in the Internet of things. *Computer Law and Security Review*, *27*(2), 133–138. https://doi.org/10.1016/j.clsr.2011.01.005

Weber, R. H. (2016). Governance of the Internet of things—From infancy to first attempts of implementation? *Laws*, *5*(3), 28. https://doi.org/10.3390/laws5030028

Whalley, J., Zhou, W., & An, X. (2009). *Chinese experience with global G3 standard-setting* (CESifo Working Paper No. 2537). Center for Economic Studies, University of Munich, Germany.

World Summit on the Information Society. (2005). *Tunis agenda for the Information Society*. Retrieved from http://www.itu.int/wsis/docs2/tunis/off/6rev1.html