



How the Internet of Things reshapes the organization of innovation and entrepreneurship

Bart Clarysse^a, Vivianna Fang He^b, Christopher L. Tucci^{c,*}

^a ETH Zurich, Department of Management, Technology and Economics, Weinbergstrasse 56/58, WEV H 311, CH-8092, Zurich, Switzerland

^b University of St Gallen, CH-9000, St Gallen, Switzerland

^c Department of Management & Entrepreneurship, Imperial College Business School, Imperial College London, South Kensington Campus, London, SW7 2AZ, UK

Digital technologies have been the driving force of business revolutions in the 2010s and 2020s, aided by technological advancements in sensors, drones, powerful computers, cloud computing, distributed ledger technology, and mobile technologies. One of the most important elements of this digital tsunami has been the Internet of Things (IoT), where smart sensors (i.e., connected sensors, as opposed to standalone sensors such as a temperature thermometer not connected to anything else) can communicate their readings of a variable of interest to a local or remote processing unit, which synthesizes and acts upon the data from the sensors. There are many types of connected sensors in use in industry, but the most common ones concern the ambient environment, such as temperature and humidity, pressure, light, movement (e.g., gyroscope), motion detectors, flow (liquid or gas), image recognition, air/water quality, and sound. The data given off by the sensors can be processed nearby (at the “edge”) if latency is an issue or can be centralized in the cloud and processed there. Indeed, IoT imbues formerly “dumb” devices with “digital intelligence,” thereby opening up a myriad of new opportunities.

The Internet of Things is one of the key elements of the Fourth Industrial Revolution, in which producers are increasingly automating their operations. The idea of devices connected with sensors to the Internet has been scaling up since the 1980s, including connecting vending machines to the Internet, but the idea predates even the 20th century: A temperature sensor on a balloon was imagined in Woolwich, UK, as early as 1843! Since the 1980s, however, relevant technologies have improved tremendously: chips have become smaller and require less power; processors have become more powerful, and RFID for wireless communication has been diffused. In addition, a technical change to the way we track device IDs was made to expand the number of possible devices connected to the Internet (cf. Ranger, 2020; Christou, 2019).

Although IoT was originally conceived of for Machine-to-Machine (M2M) communication, the biggest commercial success has been for

smart consumer-facing devices. This success, along with producer automation, has created economic value in all the major economies of the world. International Data Corporation (IDC) predicts that there will be up to 42 billion connected devices in the world by 2025, which represents six devices for every person on earth! The largest numbers of IoT devices are currently (2022) employed in smart meters for energy management and cameras/alarms for physical security, but the fastest growth is anticipated in connected buildings and connected cars. Other important areas are in home entertainment (e.g., audio, smart appliances, smart home automation), vehicle entertainment, and sports/fitness (see IoT5.net). In 2020, industries that were leading investment in IoT were (discrete) manufacturing (\$119 billion), process manufacturing (\$78 billion), transportation (\$71 billion), and utilities (\$61 billion). Across industries, worldwide spending on IoT was about \$750 billion in 2019, growing at 15% annually, and is expected to surpass \$1 trillion in 2022, according to IDC.

1. IoT, ecosystems, and business models

IoT transforms traditional value chains into digitalized ecosystems. The ecosystem around “autonomous driving vehicles” (ADV) is a case in point. The trend set by IoT puts traditional actors in industrial value chains under pressure to understand these ecosystems and to find their place in the system. For instance, ADV urges traditional OEM suppliers such as Bosch (see [Leiting et al., in this issue](#)) to revisit their role as a traditional hardware supplier to automotive manufacturers. Rather than being merely an OEM, Bosch must consider a more active role in managing an interconnected ecosystem where the traditional automotive customer plays a role while *de novo* entrants (e.g., data management startups) and diversifying entrants (e.g., telecoms such as Huawei and tech giants such as Alphabet) enter the space. Telecoms companies bring to the ADV ecosystem their long tradition in navigating through a regulated environment. In addition, IoT—in contrast to pure software

* Corresponding author.

E-mail addresses: bclarysse@ethz.ch (B. Clarysse), viviannafanghe@unisg.ch (V.F. He), christopher.tucci@imperial.ac.uk (C.L. Tucci).

URL: <http://www.imperial.ac.uk/people/c.tucci> (C.L. Tucci).

<https://doi.org/10.1016/j.technovation.2022.102644>

Received 13 March 2022; Received in revised form 3 April 2022; Accepted 10 October 2022

Available online 20 October 2022

0166-4972/© 2022 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

ecosystems—requires capital-intensive investments in both hardware and software, which must be depreciated against the long-term nature of these innovations. As Alphabet and its many acquired specialized software development companies expand, they import the California software ethos, along with its institutional logics, into this new ecosystem.

These developments have caused major shifts in industry structure, augmenting the roles played by third parties such as stock market investors and governments while rendering customers a secondary driver of impetus (cf. Bower, 1972). Electronic trading in stock markets and, relatedly, the technology hype they cause, have been shown to provide the resources necessary to get technologies and use cases off the ground (Van Lente, Spitters and Peine, 2013). Most digital companies in the US have thrived on these stock market waves and relied on their resource mobilization power. The tight coupling between digital companies and capital have created many “unicorns,” but it also separates digital companies from traditional industrial incumbents where shareholders often evaluate the quality and potential of the company based on dividends as a percentage of outstanding capital. Whereas US software unicorns bring their reliance on stock markets and valuations, Chinese telecoms bring their knowledge of lobbying and centrally steered innovations. This is not new. Government has long been known to be a main driver of long-term innovation. Examples abound, ranging from civil railways to military-inspired innovations in the aftermath of the Second World War (cf. Kaufman et al., 2003).

Despite revolutionary changes brought by IoT, most scholarly insights on ecosystems have been based on traditional understanding of digitalization (cf. Adner and Kapoor, 2010). Admittedly, the ecosystem literature has familiarized the academic and practitioner community with concepts such as platform leadership (Gawer and Cusumano, 2002), complementors and orchestrators (Adner and Kapoor, 2010) and bottlenecks (Hannah and Eisenhardt, 2018). While the literature on ecosystems has implications for interpreting the strategic decision-making of various players in the system, IoT calls for a deeper understanding of decision-making dynamics of these players. IoT ecosystems are enabled by both hardware and software. The hardware requirements are produced by the actors in the “physical” world, who are not to be taken as merely suppliers in a two-sided platform (e.g., Airbnb, Uber, or eBookers) led by an orchestrator who manages the platform. Instead, they are an endogenous part of it. Very often, the software is embedded in sensors or other hardware that they provide. Therefore, it is not clear (a) who will be a platform leader; (b) which players cause the bottleneck; or (c) what the comparable power position is. Each traditional hardware company may put forward its own component as a bottleneck, whereas newcomers may (attempt to) establish themselves as owners of bottlenecks (Baldwin, 2021).

For instance, a sensor supplier considers the sensitivity and reliability of sensors as a bottleneck whereas a data management company will consider the algorithms as a bottleneck, each attempting to provide novel solutions accordingly. The traditional vision of centralized ecosystems managed by a platform leader does not likely hold for such IoT-driven systems. In contrast, Furr and Shipilov's (2018) conceptualization of adaptive ecosystems, where not a single platform leader manages the ecosystem but typically one or more incumbents must orchestrate the development of the ecosystem, seems to be more appropriate in this case (cf. Staudenmayer et al., 2005). Such system orchestration needs different players to familiarize themselves with and respect different identities and business models. Software companies born in the heart of Silicon Valley think and operate differently from German hardware producers. A continuous effort to stimulate the different players to commit enough resources to make the ecosystem happen beyond an initial phase of excitement is also necessary. Finally, one of the main challenges is that partners in such an ecosystem do not start from a specific problem to solve, as app developers would solve the value problem of a platform like Apple's app store as a complementor. Instead, the partners must find out together which use case might be the preferred one.

The resulting ecosystem in equilibrium requires that *de novo* and diversifying entrants and incumbents search for ways of competing and cooperating with each other. In the case of autonomous driving vehicles, OEM suppliers that have traditionally focused on quality, zero error tolerance, and reliability, must be able to cooperate with software companies that emphasize lean thinking, agile development, and minimum viable products and with telecom operators that operate under a government-influenced monopoly model. These different logics may brew tensions that are difficult to reconcile. Such forms of hybrid organization need more sophisticated governance models than currently understood in the literature on hybrid forms combining social and commercial logics (e.g., Besharov and Smith, 2014). Because the institutional logics are inhabited by different individual actors, we must understand how patterns of competition or cooperation are influenced beyond the institutional level (Binder, 2007).

The research implications of IoT are both complex and exciting. They provide opportunities for researchers from different disciplines and diverse perspectives. For example, we need to understand governance systems that reallocate responsibilities and liabilities in an emerging IoT system. We also need to have better insights into the cognition of traditional players that are shaped by the institutional logics that have existed for many decades but are rapidly morphing. How do companies manage such a change process, given the dissonance that cognitive changes typically trigger? On the other hand, as *de novo* and diversifying entrants bring in new networks, new ways of communication, and new ways of valuation, social interactions amongst existing players and new entrants also warrant systematic empirical investigations. Different developments in IoT also offer possibilities to theorize about ecosystems and new digital business models that are sustainable in such ecosystems. The literature on ecosystems has evolved from considering those ecosystems as centrally managed collaborations toward defining them as organically developing sets of cooperative companies. We need more research to help understand how such “adaptive” ecosystems can be managed and how value can be appropriated (cf. Furr and Shipilov, 2018).

2. IoT and the new quest for organizational design

IoT introduces new technological and social features of organizational design, prompting changes regarding at least three critical aspects of design, which we outline here.

Locus of design. As IoT puts customers, competitors, and suppliers in a complex web (cf. Staudenmayer et al., 2005), the distributed collection, storing, and analysis of data enable local and synchronous decision-making. Such multi-party collaboration may require a network-centric rather than firm-centric design (Amit and Han, 2017). Simultaneously, much of the decision-making regarding division of labor and integration of effort (cf. Puranam et al., 2014) can now be more autonomous, taking human decision-makers largely out of the loop. Given that more and more machines are equipped with smart sensors that “talk” to each other, if human “sensors” (i.e., our sensory data) are not connected to the cloud or machines, will humans become the only remaining “dumb” elements in the system? Scholars of organizational design could explore these trade-offs and balance human-centric and machine-centric design.

Temporality of design. Due to the bounded rationality of their designers, the rhythms of organizations have been either linear or cyclical (Lefebvre, 2013). That is, traditionally, information must be gathered first, and aggregated/promulgated up the organizational hierarchy later (Brews and Tucci, 2004). Top managers then make decisions, which generate feedback and inform their future decisions. In contrast, IoT introduces a polymorphic temporal rhythm (Coletta and Kitchin, 2017), as its infrastructures and their associated networks of sensors, meters, transponders, and actuators are used to measure, monitor, and regulate the behavior of organizational agents (human or machine) in real time. Information on performance no longer needs to be aggregated and

presented to (a group of) centralized decision-makers. Instead, algorithms can make autonomous decisions for multiple feedback loops simultaneously, each of these loops having a different rhythm and each of them governed with real-time, local data. In other words, IoT has the possibility of setting in motion an “algorithm” for organizational design and organizational life.

Organizational boundaries. IoT urges us to revise answers to key questions pertaining to the boundaries of organizations. An important reason for firms to collaborate with partners in research and development has been gaining access to information (He et al., 2021). For example, Big Pharma has traditionally collaborated with hospitals that enjoy privileged access to patient data. With the prevalence of wearable medical devices and the increased sharing of personal data, firms could collaborate directly with patients in the collection and analysis of medical data. Likewise, organizational actors can collaborate across boundaries in other domains as well. Traditionally, collaboration has been built upon partners’ complementary resources, interfacing at their organizational boundary, e.g., a mouse model plus drug molecules. With IoT, collaboration may become predominantly “layered”—one partner provides physical infrastructure such as machines with sensors while the other provides data storage or analysis capacity such as cloud computing or machine learning algorithms. These changes in both the actors implicated and mode of collaboration urge scholars and managers alike to ponder the issue of trust in the design of the collaboration (Puranam and Vanneste, 2009). When there is no person behind the decision or behind the device, whom do we trust and whom do we hold accountable? A functional design of collaboration must be one that either signals *warmth* (which leads to affective trust in the actor’s intention behind collaborating) or *competence* (which gives rise to cognitive trust in the collaborators’ ability in facilitating the collaboration), or a combination of both.

Against the backdrop of this context, we summarize the different contributions to this issue in the next paragraphs.

3. Summaries of the papers in this Special Issue

This Special Issue was announced at the Academy of Management Big Data Conference in April 2018 and the International Conference on Organizing in the Digital Era in June 2019. We received 72 manuscripts by the beginning of 2020. Of these, 18 were desk rejected, and 54 entered the review process. In the end, we accepted seven manuscripts, which we feel make an important contribution to understanding this phenomenon. The articles address three main themes: (1) trends in IoT and implementation challenges; (2) assessing the impact of IoT in real-world application areas; and (3) business model implications of IoT.

We start with three articles describing **trends in IoT and implementation challenges thereof**. The article, “Discovering IoT implications in business and management: A computational thematic analysis” (Delgosha et al., in this issue), proposes an innovative explanatory sequential mixed method combining text mining and topic modeling with a qualitative approach to extract and explain knowledge from the current body of literature on IoT. To shed light on the topical structure of IoT research in the Business and Management field, the authors analyze ten topics from 347 scholarly articles. They also investigate the temporal trend of topics to display the distribution of “hot” and “cold” research topics over time. Delgosha et al. uncover the topical structure hidden in the corpus by applying thematic analysis and then identify research gaps, proposing future avenues for IoT studies in Business and Management.

The article entitled “Challenges in the implementation of IoT projects and actions to overcome them” (Martens et al., in this issue) is a qualitative study that analyzes interviews with 14 professionals and specialists involved in the application and implementation of IoT projects. The study identifies eight main implementation challenges, with seven actions used by professionals to overcome these challenges: IoT architecture; scalability, sustainability, and reliability; ensuring

security and support; information, resources, and project management; interaction of people and things; the standardization of the IoT concept; and promotion of knowledge of technologies and processes. The authors also present the relationships and co-occurrences between different challenges and actions. Based on the theory of environmental impact, the article advances a framework of problems and actions specific to the context of IoT projects, which can guide practitioners in IoT project implementation.

The next article, “Effect of Internet of Things on manufacturing performance: A hybrid multi-criteria decision-making and neuro-fuzzy approach” (Asadi et al., in this issue), discusses how IoT in manufacturing is still in its nascency, yet its benefits might be considered transformational. This study investigated the determinants of IoT adoption among manufacturers, using a hybrid ANFIS/DEMATEL approach that enabled the authors to consider interrelationships among technological, organizational, and environmental factors, and to measure their influence more accurately on performance. The findings reveal that technology competence, perceived benefits, compatibility, and technology infrastructure are the most important technological factors. Executive support, prior information technology experience, organization size, and organizational readiness are important drivers of successful IoT adoption. Finally, amongst environmental factors, external ICT support has the strongest influence on IoT adoption, followed by government support, competitive pressure, and trading partner pressure. Recommendations are provided for managers, vendors, and policymakers.

The next theme centers on **assessing the impact of IoT in real-world application areas**. “Driving social impact at the bottom of the pyramid through Internet-of-Things-enabled frugal innovations” (Park et al., in this issue), examines the role of technology-driven frugal innovation driving socio-economic impact with a focus on IoT in developing countries. Building on the process view of frugal innovation and the theory of change model, the paper evaluates the impact of IoT in bottom-of-the-pyramid markets on small enterprises in the healthcare and energy sectors, using a multiple case study approach. The paper proposes a distinction between two types of enterprises (“providers” and “enablers”) to provide a more nuanced understanding of the role of IoT on frugal innovation processes, outputs, and outcomes. Findings also uncover how IoT capabilities enhance financial viability and scalability of frugal innovations for enablers and helping providers overcome affordability and local (institutional) constraints. An elaborated framework with propositions is put forward to conceptualize the process of societal change through technology-enabled frugal innovation.

The article “Defending digital supply chains: Evidence from a decade-long research program” (Boyson et al., in this issue) is the culmination of a decade-long research project into evidence-based cybersecurity practices, and is the first statistical test of the *de facto* global standard, the U.S. National Institute of Standards & Technology’s (NIST’s) Cybersecurity Framework and its associated practice set. The article contributes to research in four literature streams: Digital Supply Chains, the Internet of Things, Cybersecurity, and Cyber-Supply Chain Risk Management. The authors focus on two cyber breach types—deficient access controls and theft—and provides initial evidence that the extent of implementation of certain elements of the NIST Cybersecurity Framework are indeed associated with fewer of these breaches when applied in real world organizational settings. This discovery provides encouragement for the further development of more effective, evidence-based cybersecurity for Digital Supply Chains.

The last two articles address **business model implications of IoT**. “The Internet of Things: Changing business models while staying true to yourself” (Leiting et al., in this issue), analyzes how Bosch—one of the largest German incumbent manufacturing firms—changed certain aspects of its business model to become an IoT provider. The study reveals how the company fundamentally altered its value proposition, and how it adapted some of its value creation and value capture mechanisms. At the same time, the firm’s history and legacy as a product-centric

company played a key role in this transformation. Through a mechanism that the authors call “imprint anchoring,” the imprinted company values that had traditionally been core to the organization provided leverage for the necessary changes of the firm’s business model in becoming an IoT provider.

Last but not least, the article “Becoming a smart solution provider: Reconfiguring a product manufacturer’s strategic capabilities and processes to facilitate business model innovation” (Huikkola et al., in this issue) analyzes longitudinally (2010–2018) six global product manufacturers considered forerunners in providing smart solutions. The study’s findings suggest that manufacturers use various realignment modes in parallel to facilitate business model innovation. The findings indicate that to create new digital capabilities, product manufacturers establish new organizational structures, processes, and routines to create and assimilate new digital knowledge as well as to sense and seize new digital opportunities. Next, product manufacturers conduct knowledge-intensive business acquisitions and establish alliances with software-based firms and startups to merge their complementary capabilities. Finally, product manufacturers release their decaying capabilities to develop new digital ones. The study’s findings reveal interesting capability-development practices that managers can benchmark when planning and pursuing such a strategic change.

4. Future research

Taken together, the articles in this Special Issue address many important topics pertaining to the technological, economic, and social implications of IoT. Building on this collection of studies, we further identify a few directions for future research. The first of these directions could focus on exploring **the link between IoT and cybersecurity**. As Boyson and colleagues show, while IoT creates a global supply chain, each link in the supply chain could be a vulnerability, thereby subject to cyber attack. On May 07, 2021, cyber-criminals shut down the pipeline supplying almost half the oil to America’s East Coast for five days. To get it flowing again, they demanded a \$4.3 million ransom from Colonial Pipeline Company, the owner. Since the arrival of COVID-19, cybercriminals have started to attack new entities, including schools, healthcare providers/researchers, and government institutions. On May 14, 2021, a cyber attack managed to cripple most hospitals in Ireland and similar attacks keep popping up in many other parts of the world. Without doubt, these two major attacks within the same month surfaced serious concerns with our digitalized, connected future, and IoT devices are notoriously insecure, for the most part not having been designed with cybersecurity in mind.

A second important area to explore is the link between **IoT and data privacy issues**. While IoT entails remote and automatic capturing and sharing of data (e.g., in healthcare), it poses increasing demands for individuals or organizations to relinquish privacy. Indeed, insights gleaned from oceans of healthcare data promise to boost health and productivity for years to come. However, should this gain come at the cost of a loss of individual privacy? Alternatively, how can we search for different modes of anonymity to protect privacy?

Third, future research should pay attention to **how IoT influences inequality in economic power** (cf. Wright and Clarysse, 2020). A major efficiency gain enabled by IoT is that machines can now perform tasks that were traditionally done by skilled individuals. However, as industries harness these technologies to improve productivity and financial performance by driving down labor costs, a structural unemployment problem may arise (George et al., 2016). In some industries, human workers, especially those with lower skill levels, face declining employability because of increasingly intelligent machines. This structural problem may in turn contribute to an expanding wealth gap between socioeconomic classes. Inequality amongst individuals aside, IoT also further tilts the power balance between large corporations (e.g., Alphabet) and small- and medium-sized companies. One potential scenario is that with massive existing networks of customers and suppliers,

large conglomerates could build and harness IoT much faster and more effectively than new entrants or smaller players, reinforcing the market power of “giants.” An alternative scenario, however, is that IoT could indeed break data monopoly power as more individualized data sources become available outside the existing networks of those “giants.”

Fourth, an intriguing avenue of research is at the **nexus of IoT and digital business models**. IoT implies a decentralized network in which partners that develop software, produce hardware, and manage data need to work together as equals. These different partners have different legacies, identities, and business models. It is unlikely one of them will be able to act as a platform leader. Moreover, most of these collaborations also include public partners that represent societal goals that might not be in line with the commercial goals of the private partners. The core of the software companies has roots in the Bay Area or China, whereas the traditional hardware manufacturers are to be found in many more geographic areas. This introduces diverging goals and cultural values. Research is needed to explore how such ecosystems, with time horizons often exceeding a time to profitability of over five to ten years, can be set up and become sustainable. This requires new insights in strategy, organizational design, and organizational behavior.

Finally, a promising direction to explore is **the growing interdependence between IoT and other advanced technologies**. For example, when IoT is combined with nanotechnology (cf. Balasubramaniam and Kangasharju, 2013), what does a nanoscale IoT system imply? (Ever more minute scale of each individual data point vs. a large and ever-expanding data network ...) Similarly, when IoT is further combined with blockchain technology, how does the result change the organization of production activities and data collaboration (cf. Luminéau et al., 2021)? As a subset of distributed ledger technology, blockchain allows digital data to be stored in a cryptographically secured and decentralized manner. When IoT devices are combined with blockchain technology, a network’s ability to collect and digitize informational, physical, and financial flows across firm boundaries may be transformed (Lacroix et al., 2022). Future research could explore the opportunities and challenges brought by such transformation, for incumbent/legacy institutions, new entrants, and for innovative ways of collaboration among stakeholder groups for whom collaboration used to seem impossible.

In conclusion, this Special Issue kick-started efforts to translate the challenges of IoT, which is at the core of digitalization, into a business challenge. Most papers in the Special Issue are the result of a collaboration between technical professors who are mostly interested in the practicalities of implementing IoT-related technologies and business school professors who identify the business model and ecosystem challenges as the most important ones while the underlying technologies are seen as instrumental. Bridging these two views through cross-disciplinary research is needed to add relevance to the management view while at the same time adding theoretical depth to the technology view. This Special Issue offered an excellent opportunity to do just this.

References

- Adner, R., Kapoor, R., 2010. Value creation in innovation ecosystems: how the structure of technological interdependence affects firm performance in new technology generations. *Strat. Manag. J.* 31 (3), 306–333. <https://doi.org/10.1002/smj.821>.
- Amit, R., Han, X., 2017. Value creation through novel resource configurations in a digitally enabled world. *Strateg. Entrep. J.* 11 (3), 228–242. <https://doi.org/10.1002/sej.1256>.
- Asadi, S., Nilashi, M., Iranmanesh, M., Hyun, S.S., Rezvani, A., 2021. Effect of Internet of Things on manufacturing performance: a hybrid multi-criteria decision-making and neuro-fuzzy approach. *Technovation*, 102426. <https://doi.org/10.1016/j.technovation.2021.102426>.
- Balasubramaniam, S., Kangasharju, J., 2013. Realizing the internet of nano things: challenges, solutions, and applications. *Computer* 46 (2), 62–68. <https://doi.org/10.1109/MC.2012.389>.
- Baldwin, C.Y., 2021. *Design Rules, vol. 2. Harvard Business School (Chapter 16), Capturing Value by Controlling Bottlenecks in Open Platform Systems, Harvard Business School Research Paper Series*, 20–054.

- Besharov, M.L., Smith, W.K., 2014. Multiple institutional logics in organizations: explaining their varied nature and implications. *Acad. Manag. Rev.* 39 (3), 364–381. <https://doi.org/10.5465/amr.2011.0431>.
- Binder, A., 2007. For love and money: organizations' creative responses to multiple environmental logics. *Theor. Soc.* 36 (6), 547–571. <https://doi.org/10.1007/s11186-007-9045-x>.
- Bower, J.L., 1972. *Managing the Resource Allocation Process: A Study of Corporate Planning and Investment*. Irwin, Homewood.
- Boyson, S., Corsi, T.M., Paraskevas, J.-P., 2021. Defending digital supply chains: evidence from a decade-long research program. *Technovation*, 102380. <https://doi.org/10.1016/j.technovation.2021.102380>.
- Brews, P.J., Tucci, C.L., 2004. Exploring the structural effects of internetworking. *Strat. Manag. J.* 25 (5), 429–451. <https://doi.org/10.1002/smj.386>.
- Christou, L., 2019. History of IoT: from Idea to an Industry Approaching \$1tn. <https://www.verdict.co.uk/history-of-iot/>.
- Coletta, C., Kitchin, R., 2017. Algorithmic governance: regulating the 'heartbeat' of a city using the Internet of Things. *Big Data & Society* 4 (2). <https://doi.org/10.1177/2053951717742418>, 2053951717742418.
- Delgosha, M.S., Hajihedari, N., Talafidaryani, M., 2022. Discovering IoT implications in business and management: a computational thematic analysis. *Technovation*, 102236. <https://doi.org/10.1016/j.technovation.2021.102236>.
- Furr, N., Shipilov, A., 2018. Building the right ecosystem for innovation. *MIT Sloan Manag. Rev.* 59 (4), 59–64.
- Gawer, A., Cusumano, M.A., 2002. *Platform Leadership: How Intel, Microsoft, and Cisco Drive Industry Innovation*, vol. 5. Harvard Business School Press.
- George, G., Howard-Grenville, J., Joshi, A., Tihanyi, L., 2016. Understanding and tackling societal grand challenges through management research. *Acad. Manag. J.* 59 (6), 1880–1895. <https://doi.org/10.5465/amj.2016.4007>.
- Hannah, D.P., Eisenhardt, K.M., 2018. How firms navigate cooperation and competition in nascent ecosystems. *Strat. Manag. J.* 39 (12), 3163–3192. <https://doi.org/10.1002/smj.2750>.
- He, V.F., von Krogh, G., Sirén, C., Gersdorf, T., 2021. Asymmetries between partners and the success of university–industry collaborations. *Res. Pol.* 50 (10), 104356.
- Huikkola, T., Kohtamäki, M., Ylimäki, J., 2022. Becoming a Smart Solution Provider: Reconfiguring a Product Manufacturer's Strategic Capabilities and Processes to Facilitate Business Model Innovation. *Technovation*.
- Kaufman, A., Tucci, C.L., Brumer, M., 2003. Can creative destruction be destroyed? Military IR&D and destruction along the value-added chain. *Res. Pol.* 32, 1537–1554.
- Lacroix, R., Tucci, C.L., Seifert, R., 2022. Blockchain of Things Sweet Spots for Lean and Agile Supply Chains. Working Paper. EPFL College of Management, Lausanne, Switzerland.
- Lefebvre, H., 2013. *Rhythmanalysis: Space, Time and Everyday Life*. Bloomsbury Publishing.
- Leiting, A.-K., de Cuyper, L., Kauffmann, C., 2022. The Internet of Things: Changing Business Models while Staying True to Yourself. *Technovation*.
- Lumineau, F., Wang, W., Schilke, O., 2021. Blockchain governance—a new way of organizing collaborations? *Organ. Sci.* 32 (2), 500–521. <https://doi.org/10.1287/orsc.2020.1379>.
- Martens, C.D.P., da Silva, L.F., Silva, D.F., Martens, M.L., 2021. Challenges in the implementation of internet of things projects and actions to overcome them. *Technovation*, 102427. <https://doi.org/10.1016/j.technovation.2021.102427>.
- Park, S., Rosca, E., Agarwal, N., 2021. Driving social impact at the bottom of the Pyramid through the Internet-of-things enabled frugal innovations. *Technovation*, 102381. <https://doi.org/10.1016/j.technovation.2021.102381>.
- Puranam, P., Alexy, O., Reitzig, M., 2014. What's "new" about new forms of organizing? *Acad. Manag. Rev.* 39 (2), 162–180. <https://doi.org/10.5465/amr.2011.0436>.
- Puranam, P., Vanneste, B.S., 2009. Trust and governance: untangling a tangled web. *Acad. Manag. Rev.* 34 (1), 11–31. <https://doi.org/10.5465/amr.2009.35713271>.
- Ranger, S., 2020. What Is the IoT? Everything You Need to Know about the Internet of Things Right Now. ZDNet. <https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/>.
- Staudenmayer, N., Tripsas, M., Tucci, C.L., 2005. Interfirm modularity and its implications for product development. *J. Prod. Innovat. Manag.* 22 (4), 303–321.
- van Lente, H., Spitters, C., Peine, A., 2013. Comparing technological hype cycles: towards a theory. *Technol. Forecast. Soc. Change* 80 (8), 1615–1628. <https://doi.org/10.1016/j.techfore.2012.12.004>.
- Wright, M., Clarysse, B., 2020. Technology entrepreneurship and shaping industries. *Acad. Manag. Discov.* 6 (3), 355–358.