Proceedings of the 52nd Hawaii International Conference on System Sciences | 2019

Towards an Internet of Things society: Perspectives from government agencies in Sweden

Juho Lindman
University of Gothenburg
juho.lindman@ait.gu.se

Ted Saarikko
University of Gothenburg
ted.saarikko@ait.gu.se

Abstract

Digitalization in general, and the Internet of Things (IoT) in particular, is dramatically transforming societies, affecting both industry and the public sector. Government agencies have a role to play in how successful distribution and implementation of IoT technologies are. We conducted an explorative, qualitative study based on 16 interviews with key respondents from government agencies in Sweden to discover the public sector agencies' current maturity. We focused on society as a whole and drilled down into individual sectors: energy, food, transportation, health care, financial services, information and communication, and security. Governance challenges are identified related to the complex ecosystem interplay of public and private actors, including lack of common guidelines, sparsity of expertise, and each respective agency's evolving roles in an increasingly connected society.

1. Introduction

Increasing engagement with digital technology in the public sector has been traditionally viewed through roughly two separate lenses: either as a means to increase existing process or as a way to radically transform the public sector [1]. For instance, the Internet of Things (IoT) can promote "smart" communities and more efficient use of government resources, for example, by using autonomous sensors to control infrastructure [2], manage logistics [3], and monitor the environment [4]. These capabilities promise new forms of governance that draw upon the possibilities of developing technologies and connectivity. Increasing the IoT's penetration is one part of an emergence of what is considered the next generation of government infrastructure [5], which is sometimes referred to as government 3.0 [6]. These new technologies afford: i) efficiencies of internal processes/practices/services and optimization of resource consumption; ii) evidence-based decision support drawing on these technologies (big data, societal simulation); and iii) use of internal and external resources in public service provisioning [6]. Government activities can play a role in this development and influence how IoT transforms society via regulation, investment, and endorsement.

However, IoT applications on this scale are typically larger and involve heterogeneous sets of actors where not all participants are public organizations; therefore, governing this mix is more difficult than more traditional applications of IT in government services, such as e-government [6]. The scope and technical diversity of the IoT requires various capabilities and involves stakeholders who need to be brought together, which poses new challenges for governing and supervising these services [7, 8]. Moreover, although IoT applications vary significantly between application domains, they are dependent on the rules and regulations established by government agencies or multinational institutions, such as the General Data Protection Regulation, established by the European Union [9].

Maturity and maturity models have been a common topic of research in many areas, such as e-goverment [10], industry 4.0 [11], and general IT management [12]. The United Nations' definition [13, p.1] of e-government highlights "*utilizing the internet and the WWW for delivering government information and services to citizens.*" Emergence of private actors and networks in the service provision is a common theme across the work carried out in this field. Still, for example, a survey of eGovernment literature published between 2000 and 2010 [14, p. 23] includes calls for novel models *"to meet the contemporary and future challenges of eGovernment."*

URI: https://hdl.handle.net/10125/59774
ISBN: 978-0-9981331-2-6

We heed this call in this paper and argue that government 3.0 and its subset IoT change these dynamics, allowing for broader T engagement and opening fertile ground for new research. The long-term aim of our research effort is to build a new maturity model for IoT in government. This paper is a necessary first step in the effort to determine the baseline of government 3.0 for these efforts. For the purpose of clarification, we perceive *maturity* as a composite property consisting of expertise related to the IoT, ability to apply (or guide the application of) the IoT, and perceived challenges in IoT governance.

Drawing upon the promises of government 3.0, the objective of this paper is to offer insights into the current state of Swedish government agencies and their ability to leverage the IoT to manage internal resources (e.g., skills, assets, and processes) and their commitment to serve external stakeholders (e.g., citizens and private companies). Therefore, we state our research question thusly: *What is the current level of IoT maturity among Swedish government agencies?*

2. Background: The Internet of Things

2.1 Definition and possibilities

The IoT does not depict a specific technology per se; rather, it denotes a wider movement toward connecting individual components, commercial products, or whole environments to local or global telecommunications networks [15, 16]. A working definition is provided by Miorandi et al. [16, p. 1497]: "*The term 'Internet-of-Things' is used as an umbrella keyword for covering various aspects related to the extension of the Internet and the Web into the physical realm, by means of the widespread deployment of spatially distributed devices with embedded identification, sensing, and/or actuation capabilities."*

Manifestations of the IoT range from basic monitoring and positioning of physical assets to more advanced applications that extend product or system applicability by virtue of malleable, reprogrammable digital technology [17]. IoT applications are visible across all domains of society [18].

Research has thus far favored technical topics [19], limiting our understanding of the IoT's managerial, social, and economic implications. Practitioners and academics quite often refer to the IoT as though it represents a single, cohesive body of knowledge. That is, however, hardly the case. It would be more accurate to describe it as a heterogeneous collection of various technologies that can be used to link a wide range of various artifacts, such as networks, products, components, and small tags [15].

Hence, it is inaccurate to consider the IoT as a technology, infrastructure, or standard; rather it should be thought of as a design perspective or a functional extension of existing devices. The ambition to combine physical machinery with remote connectivity is by no means a novelty. However, the cost and complexity associated with such endeavors have limited its operationalization to large-scale industrial installations, where the cost of installing custom-designed sensors, networks, and computers is dwarfed by the enormous costs associated with maintenance and repairs [20].

The diversity of technologies related to the IoT, including sensory equipment, short-range data transfer, long-range communication, storage, analysis, and utilization, have prompted interest in platforms that can mitigate much of the complexity and permit various actors to focus on their own contributions without disentangling an entire infrastructure (e.g., [21, 22]). Borgia [18] describes in detail how IoT service platforms aid the management of information flow and hide complexities of the underlying technical architecture from the end user.

2.2. Perspectives and applicability

As the IoT is approached more as a loosely defined perspective or phenomenon, it naturally follows that academic expertise on the topic is often divided regarding the relative importance of certain key concepts. Our position is one of agreement with Whitmore et al. [19, p. 269] who conclude that "IoT research will need to broaden into the fields of management, operations, law, economics, and sociology, among others."

The ostensible novelty and increased attention associated with the IoT does not stem from the development of any single technical innovation or sudden realization that connected products offer new affordances but from the fact that the associated technical and financial barriers have gradually crumbled. The ongoing miniaturization of technical

equipment brings with it computers and sensors that are smaller, cheaper, and require less power. The cost of transferring data between various locations has plummeted as wired and wireless networks grow ever more available. By using customized software (called middleware), we can link various types of networks and machinery and thus provide seamless connectivity despite an increasingly diverse range of devices and applications [15, 23].

Urban and rural actors in the public sector can leverage the IoT to suit their individual priorities and challenges. Large cities can utilize citywide sensors to monitor conditions in certain areas or throughout the city in real time, providing accurate and up-to-date information in the interest of public service, such as traffic management, and public safety, such as air quality [24]. Rural municipalities can benefit from new technical standards developed specifically for IoT applications. One example is the low-power wide-area network [25], which is specifically designed for the exchange of data in short, efficient bursts over long distances between connected devices. Equipment utilizing this standard can be placed several miles away from any central receiver and still operate for a decade on battery power, permitting coverage of large areas on a small or moderate budget.

Underlying IoT technologies are typically not developed by any single actor but in ecosystems, clusters, and sectors where a number of various actors combine their intellectual and material resources [26]. In addition to device manufacturers and commercial service providers, public sector agencies play key roles in both supporting (e.g., via infrastructure) and limiting (e.g., via rules and regulations) technology diffusion.

3. Methodology

The empirical part of our research may be characterized as an explorative, qualitative study. In keeping with interpretive methods often used in IS research [27], our intention is to provide an understanding of how information artifacts and information systems interact with their surroundings [28]. Specifically, we wish to understand level of IoT maturity in government agencies. A qualitative approach is motivated by the multiplicity and complexities of government responsibilities, together with variations in technology's relative significance in various contexts. Moreover, a qualitative approach permits the elicitation of informed answers, enabling "*in-depth studies about a broad array of topics […] in plain and everyday terms*" [29, p. 6].

3.1. Research context

Sweden provides an interesting context for this study, as it rated #2 among 60 countries in a 2017 digital competitiveness survey [30], indicating a high degree of maturity regarding the acceptance of digital innovation and e-government services. As such, situating the study in a Swedish context permits us to focus on knowledge and experience pertaining to digital technology and services rather than remedial issues, such as availability of IT infrastructure.

3.2. Data gathering

We approached the participating agencies (see Table 1) either by directly contacting IoT-knowledgeable employees or by approaching the respective agency, outlining our interests and requesting that our inquiry be routed to a suitable individual or department. In keeping with our study's explorative nature, we applied "snowball sampling," whereby a respondent is not simply asked to respond to questions but also to provide suggestions for additional interviews or secondary sources of data.

As this study was situated in a Swedish context, we sought out agencies that engage with any of the seven sectors that provide critical societal functions according to the Swedish Civil Contingencies Agency: energy, food, transportation, health care, financial services, information and communication, and security. Altogether, we conducted 16 interviews with individuals from 13 agencies. The number of respondents participating in each interview varied between one (13 interviews) and two (3 interviews). Interviews took place between November 2017 and February 2018.

Interviews were conducted via Skype or telephone per agency policy or respondent preferences. The interviews varied in length between 30 and 60 minutes, depending on the respondent's role and insight. Most interviews (15 out of 16) were recorded and subsequently transcribed. One interview was

recorded via notes rather than audio recording, as the respondent did not wish to be recorded.

Given the disparity of participating agencies, we outlined a semi-structured interview protocol based on six areas of inquiry in keeping with our research question and a review of extant IoT literature: 1) IoT as a term, 2) the IoT as an area of expertise, 3) functionality and possibilities, 4) current and future applications, 5) challenges and risks, and 6) resources and security measures.

3.3. Data analysis

Analysis followed an interpretive approach [27] whereby empirical data provided by the respondents were interpreted based on the researcher's theoretical understanding of the research topic at hand. Data analysis was conducted in three steps. First, the six areas of inquiry served as a heuristic to identify relevant statements the respondents made. This initial analytical step was supported by the use of ATLAS.ti, a software tool frequently used in qualitative research to code data. Microsoft Excel was used for additional tasks related to presentation and overview of data and results.

Second, we aggregated respondent statements based on sector (see table 1) in search of common themes and perspectives among agencies with similar areas of responsibility. The results of this step of the analysis are presented in chapter 4. The final results of our sector-based analysis were communicated back to the respondents with an invitation to review and comment upon our findings.

Third, we aggregated the results of the analyses of individual sectors to discern the current readiness for and perceptions of IoT within Swedish government agencies as a whole. We present and discuss outcomes of this final analytical step in chapter 5.

4. Findings

We present the results of our study based on the sectors presented in table 1.

Table 1. Participating agencies.

Sector	#	Agency	Respondent role
Energy	1	Energy Agency	Senior Adviser, Research and Innovation
	2	Energy Agency	Program Manager, Energy Analysis
Food	3	National Food Agency	Head of IT Services & Team Manager, Operational Governance
Transportation	4	Transport Administration	Lead IT Architect
	5	Transport Administration	Enterprise Architect Infrastructure
Health care	6	eHealth Agency	Business Developer
	7	eHealth Agency	Chief Security Officer
	8	Association of Local Authorities and Regions	Program Manager, Dept. of Digitalization
Financial services	9	Tax Agency	Head Digital Co-development & Business Developer
	10	Social Insurance Agency	Innovation Lead
Information and communication	11	Data Protection Authority	IT security Specialist
	12	Post and Telecom Authority	Senior Policy Adviser
Security	13	Defense Research Agency	Researcher
	14	Mapping, Cadastral, and Land Registration Authority	Application Architect
	15	Defense Materiel Administration	CIO & Head of IT Systems Logistics
	16	Police Authority	Specialist, Swedish Cybercrime Center

4.1. The energy sector

Our study shows that government agencies in charge of oversight see clear potential in the IoT. Indeed, they continually fund and promote research into technologies that can enhance the national energy infrastructure's robustness and efficiency. However, the energy sector exhibits a wide disparity in its constituent actors, making IoT diffusion a challenge.

Much of the energy sector comprises regional actors that typically operate on limited budgets that are often burdened with a significant technological debt from gradually improving, upgrading, and replacing individual systems as motivated by operational necessity rather than long-term strategy. While they do in some cases utilize connected systems, they struggle to provide adequate security. On the other hand, national and international enterprises can draw upon their considerable resources to develop cohesive, long-term strategies for delivering secure, efficient solutions. Given the heterogeneity, large private actors rather than agency policy or guidelines thus far provide IoT diffusion in the energy sector.

4.2. The food sector

Overall, the food industry is slow to adopt digital tools to support inspection and oversight. This is partly due to EU regulations that require the physical presence of a certified inspector. Respondents also cited a conservative culture that is slow to adopt new technologies. Hence, oversight is almost entirely based on manual inspections, and inspection protocols are compiled annually, leaving the agency with massive amounts of reports that take months to process and review. Therefore, government oversight is currently slow to detect deviations from acceptable standards or practices.

Contrary to the production of foodstuffs, retail and distribution is subject to digitalization and rapid change. Customers increasingly order locally sourced foodstuffs online and have them delivered directly to their door. Government agencies face significant challenges in adapting to these novel business models, as manual inspections are not feasible in the face of massive online retail. A greater presence of "smart" devices that monitor areas where food is packaged and stored could be part of broader interagency response to shifting industry practices.

4.3. The transportation sector

Our study reveals a transportation sector that has been actively engaging for many years with technologies and practices that fall under the general paradigm of the IoT. The transport administration has been relying upon various forms of technology to supervise road and rail safety and maintenance for many years.

However, a long history of using technology also brings a heterogeneous patchwork of systems. There are significant challenges associated with integrating systems, products, and components delivered by various suppliers given the overall lack of shared technical standards. In addition, supplier-defined protocols often exhibit poor security features and could be exploited for unauthorized access to individual devices or even larger systems. Hence, the agency featured in our study handles the issue by maintaining a large, in-house IT staff who can customize equipment before use. Nevertheless, a favorable long-term strategy is to work with suppliers and convince them to adopt or help develop secure protocols and standardized interfaces. Long-term contracts are a possible incentive, providing a tangible motive for suppliers to improve their products.

There is, however, a disparity in the level of standardization present in railroad and road networks. Railroads have historically been tightly regulated, and the underlying infrastructure is therefore relatively homogeneous. In comparison, roads and roadside technologies are much more diverse, as infrastructure has expanded on a project-by-project basis, forming a patchwork. Hence, it is presently much more feasible to leverage the IoT to oversee the Swedish railway rather than roads.

4.4. The health care sector

Respondents from the health care sector explain that care for outpatients and elderly citizens stands to gain significantly through adoption of IoT-oriented technologies. Connected "smart" devices can provide easy, round-the-clock access to health care personnel via a simple alert button. Moreover, digitized medical

tools can enable citizens to monitor their own blood sugar levels or blood pressure in the comfort of their homes without extensive medical training. The results of the respective tests can then be logged and presented to the patient or medical personnel.

However, the health care sector—perhaps more so than the other sectors—is bound by limitations imposed by legal restrictions as well as ethical considerations on how personal information may be handled. One responded cited that a large eHealth initiative intended to permit outpatients the freedom to manage their own data was halted by a court order shortly before it was scheduled to go online. Hence, the current uptake on IoT is limited to individual tools that provide incremental improvements.

4.5. The financial services sector

The financial sector is not spared the forces of digitalization, as we increasingly use credit cards or smartphones equipped with near-field communication (NFC) or radio frequency identification (RFID) technology to make purchases. Furthermore, cryptocurrencies like Bitcoin, which, as of December 2017, is traded on two exchanges, are gaining legitimacy.

The main challenge for agencies set to regulate the financial sector is simply to remain relevant in the face of these novelties. Our study hints at an emerging gulf in "digital maturity" based on how we conduct ourselves in our private lives versus how we behave in our professional lives. As private citizens, we are relatively quick to adopt novel financial services, but we still rely on traditional financial institutions and forms of payment in professional contexts.

Government agencies tasked with overseeing the financial sector have to accommodate both ends of the spectrum: traditional financial structures and new digital innovations. Any blind spot could yield marketplaces or even whole economies that operate without oversight, either intentionally (i.e., for criminal activity) or through an uninformed citizenry. One respondent in our study cautioned against a "democracy-deficit," where citizens do not perceive government agencies as relevant in a modern economic landscape. One way to address the situation is to develop suitable legal and technical interfaces that reconcile existing laws and tax codes with new currencies and forms of payment. This step will facilitate new services that comply with existing financial regulations.

4.6. The information & communication sector

Agencies overseeing the information and communication sector also find themselves responding to an influx of digital technologies. Organizations in private and public sectors seek information regarding what is and is not permissible and often end up posing their inquiries to the agencies in charge of oversight. As the IoT is poised to encompass millions (or even billions) of connected devices distributed across multiple societal sectors, we may surmise that the issue of uncertainty is not going away any time soon. Our study suggests that while plenty of enthusiasm surrounds technical novelties, our legal frameworks and knowledge among users exhibit a dearth of maturity. New technical paradigms, such as the IoT and, before that, cloud computing, tend to cause confusion regarding how regulations should be applied. However, respondents in our study stressed that people generally do not want more laws; they want more guidance in applying existing laws.

4.7. The security sector

It is worth noting that security was raised as a major concern across all sectors featured in our study. However, we also interviewed agencies that focus specifically on security (e.g., law enforcement and national defense).

A respondent from law enforcement highlighted that criminal activity is subject to digitalization just like any other activity or process. Criminals can utilize technology to commit theft, fraud, or worse. Crime prevention involves two distinct steps. The first step is to build devices that are harder for unauthorized personnel to misappropriate (i.e., hack). Government agencies can influence developers and retailers either by imposing explicit requirements (i.e., in public procurement) or by facilitating a dialogue between actors in the public and private sectors. The second step concerns how technology—even if legally acquired—can be applied as a tool for various forms of criminal activity. For an analogy, a kitchen knife may be purchased and used to prepare a meal. It may

also be used as a weapon. Therefore, there is a need to work proactively rather than reactively in developing and evaluating various scenarios where technology can be used to society's or its citizens' detriment.

Finally, as our society becomes more digitalized, government agencies also work to develop standards and routines for management of information in at the organization and department levels. When faced with major incidents, agencies often have to work together and coordinate their efforts under challenging circumstances. Therefore, although the need for regulatory standards for various sectors arose in multiple interviews, a need also exists for standards that regulate interagency activities under various conditions.

5. Discussion

Following the presentation of results from individual sectors, we will now discuss cross-sector results based on the categories outlined in relation to our research question: the IoT as an area of expertise, its applicability, and challenges in governance.

5.1. The IoT as an area of expertise

During the course of our study, we asked the respondents whether their respective agencies had adopted any official definition of the IoT or whether it was viewed as a distinct area of expertise. The results were conclusive because no agency featured in our study has developed or adopted an official view on the definition or scope of the IoT. Individual respondents provided disparate views on how new technologies can benefit society [6] related to their own area of interest. Some were very specific, such as respondents from the transportation sector, where agencies work with specific connected devices and rely on accurate data to supervise roads and railway networks. In contrast, respondents from the security sector agreed that the IoT encompasses just about anything that can be connected to the Internet.

Furthermore, no agency featured in our study considers the IoT a distinct area of knowledge or expertise. The diverse and disparate knowledge resources [16] that form the basis for IoT application or oversight are either missing or distributed across the agency with little or no coordination. Respondents from the agency overseeing the food sector explicitly stated that it would take a significant investment in technology and labor to accommodate major technical innovations. Other agencies (e.g., in the energy sector) state that they possess relevant knowledge resources on an informal basis owing to individual employees with a personal interest or relevant working experience. Overall, IoT-related skill sets are most prevalent and cohesive in the transportation, information and communication, and security sectors, albeit from various perspectives. Agencies in the information and communications sector do not apply connected devices but are often tasked with investigating the legality or ethical consequences of new technologies as they proliferate into different domains [18]. Therefore, the IoT can be viewed as "more of the same" rather than an innovation. The security sector offered a similar view, albeit from a technical perspective. Respondents did not see connected devices as new phenomena as much as a variant on the existing issue of safeguarding systems to prevent unauthorized access. Moreover, several agencies try to consider not just the systems' integrity but also the ramifications of unauthorized access. That is, it is not merely a matter of safeguarding digitized information, such as medical histories or financial transactions [19], but also considering the real-world ramifications of a connected product, like a vehicle, being manipulated or controlled by malicious forces.

5.2. Applicability of the IoT

We asked respondents if they could offer us any examples of how they apply the IoT today and describe the possibilities and advantages they perceive regarding connected devices. Overall, use cases pertaining to IoT are poorly developed among participating agencies.

Our findings show that the transportation and security sectors offered the most concrete use cases pertaining to IoT. Respondents from the Transport administration described how the agency maintains 700 automated weather stations that gauge local conditions along the national road and railway infrastructure. In addition, railroad exchanges are fitted with sensors that monitor their positions and operational status. Respondents from the security sector also described how law enforcement utilizes

automatic number plate recognition (ANPR) to scan passing vehicles' plate numbers. The system flags cars associated with legal infractions (e.g., reported as stolen) and alerts law enforcement officers. Additionally, agencies have installed specialized microphones in areas where crime is especially prevalent. The microphones register specific sounds associated with criminal activity (e.g., breaking glass or gunshots) and notify law enforcement if there is reason to believe a crime is in progress.

Looking beyond extant applications and into applicability, responses were unanimously positive but often vague, alluding to the possibility of leveraging cheaper and more versatile devices to provide more data and help the agency perform its assigned tasks. Respondents that saw short-term, operational benefits for their organizations were generally able to provide more tangible use cases. For instance, the agency tasked with overseeing the food sector routinely inspects facilities where food is prepared, stored, or transported. This process is time-consuming, as such facilities are often located in remote locations, forcing inspectors to spend several hours of their working day traveling to and from a site. Automating certain aspects of routine inspections via connected devices would free up a considerable amount of time, which could be devoted to other (nonroutine) tasks. Furthermore, the agency currently receives reports on manual inspections at the end of the year in the form of huge data files that take months to compile and analyze. The lag between inspection and response can stretch up to 15 months. Automating parts of the inspection process could significantly improve the quality of oversight.

Another possibility—voiced in the transportation sector—is to adopt crowdsourcing to generate information. Each train, truck, and, to an increasing extent, automobile, carries a significant amount of on-board sensors and sophisticated systems that asses the vehicle's condition and surroundings, such as vibrations, temperature, rotational speed of wheels, local weather conditions, traffic congestion, road conditions, or wear and tear on the rail. Access to data generated by each vehicle travelling by road or rail in Sweden could provide a wealth of information to support day-to-day operations and long-term statistical analyses. Realizing this idea on a large scale would, however, require extensive reviews of current legal frameworks and development of palatable incentives to share data.

Our study suggests that IoT could economize on resources yet still *improve* the quality of the results, sentiments that are especially pronounced in the healthcare, transportation, and food sectors, where human resources are stretched thin in the face of increasing workloads.

5.3. Challenges in governance

Finally, we asked the respondents about risks and general challenges associated with governing the IoT in their respective agencies. Although details differ, the situation facing the energy sector (see chapter 4.1 above) is emblematic of all sectors featured in our study. That is, embracing the IoT could *potentially* bring many advantages, but will *certainly* require significant investments in terms of time, funding, and expertise [7, 23].

Government agencies all have areas of responsibility and certain goals that they strive to achieve. And, although investments in the IoT may facilitate the accomplishment of long-term agency goals, they may prove difficult to justify in the short term unless a clear political mandate or motive moves them in that direction. Several respondents also claimed legal restrictions limited the IoT's proliferation, as the legal framework is either obsolete or unclear regarding technical innovations. The General Data Protection Regulation [9], which is intended to protect personal integrity, was viewed as hindering the adoption of IoT while society as a whole evaluates its implications.

The two most-cited technical concerns in our study were security risks and a lack of standardization. The former is an immediate deal breaker for many agencies, especially in the security sector. Although connected equipment could feasibly provide many advantages (e.g., predictive maintenance [26]), the risks associated with remote connectivity are simply unacceptable for most law enforcement and military applications. Any remote interface is, essentially, another possible way to render a system useless.

The issue of standardization is also a source of concern, as manufacturers of connected devices often prioritize time to market and utilize proprietary protocols that often offer poor security. User

information or passwords may be sent without any encryption whatsoever, making interception by third parties easy. The need for secure interfaces is especially germane for IoT devices, as they are more autonomous than personal digital devices, such as desktop computers and smartphones. IoT devices operate with little or no direct involvement by people, meaning that a breach of security may go unnoticed for comparatively longer periods of time. The lack of standardization and secure protocols were emphasized by respondents in agencies that already have experience with connected devices (e.g. the Transport administration) as a continuous source of concern and a driver of costs. While using connected devices to supervise infrastructure has clear long-term benefits, the lack of standardization and mature communication protocols means that agencies have to bear the short-term cost of integrating (or even upgrading) individual connected devices into a cohesive system, severely hampering the appeal of IoT in many situations.

6. Limitations and future research

In our study, we interviewed one or two respondents from just 13 agencies, and the selection of respondents was often based on convenience sampling and snowball sampling. Therefore, our study does not represent a true cross section of Swedish government agencies. However, we believe that our approach has given us access to the individuals with the most insight and interest in the IoT from each respective agency. In addition to the results presented and discussed in chapters 4 and 5, our study also suggests areas for futures studies of the public sector IoT.

First, this study provides a snapshot from government agencies in a Swedish context. However, research into the IoT must consider the international context, as new technologies and innovative applications are not limited to any single country or region. Therefore, we see a significant need for comparative studies for the purposes of international benchmarking, identification of success factors, and even deeper understanding of how social, legal, and technical systems interact under various circumstances.

Second, for all its potential, the IoT also poses a number of challenges, including unforeseen security risks that need to be mitigated for critical societal services [8]. Some of these risks are strictly technical and limited to the integrity of new equipment. However, connected systems that combine digital and physical components require a socio-technical approach wherein stakeholders consider real-world consequences of hacked products (e.g., automobiles or traffic control systems). The autonomous nature of connected devices opens up new attack vectors that are difficult to foresee due to the underlying technology's interconnected nature, and we need to develop mechanisms to mitigate these risks.

Finally, the IoT represents a highly diverse area of research and practice that encompasses multiple stakeholders who contribute their own expertise but also bring their own agendas. The rift is especially large between public and private sector enterprises, which often have different metrics for success (i.e., profit versus public service). Future research needs to develop platforms and governance mechanisms that promote and simplify public-private collaborations in IoT ecosystems.

7. Conclusions

We have presented an overview of current perspectives of the IoT from 13 Swedish agencies distributed across seven societal sectors. We see significant differences in the level of maturity as current expertise, application, and governance of IoT are predominantly reactive and based on operational necessity rather than any proactive, long term-strategy. While a few agencies, notably the Transport administration, are quite accustomed to working with connected devices, other agencies are still a long way from the vision of government 3.0. These differences could, in time, yield a patchwork of inconsistent policies that could impede the formation of national initiatives and ICT-enabled governance. However, these inconsistencies also provide opportunities to promote structures that facilitate interagency knowledge transfer and learning. Based on our findings, we call for future research to measure and benchmark IoT maturity in government agencies.

8. References

[1] A. Cordella, and C. M. Bonina, "A public value perspective for ICT enabled public sector reforms: A

theoretical reflection", Government Information Quarterly, Vol. 29, No. 4, 2012, pp. 512-520.
[2] F. Leccese, M. Cagnetti, and D. Trinca, "A smart city application: A fully controlled street lighting isle based on Raspberry-Pi card, a ZigBee sensor network and WiMAX", Sensors, Vol. 14 No. 12, 2014, pp. 24408-24424.
[3] P. Neirotti, A. de Marco, A. C. Cagliano, G. Mangano, and F. Scorrano, "Current trends in Smart City initiatives: Some stylised facts", Cities, Vol. 38, 2014, pp. 25-36.
[4] H. Schaffers, N. Komninos, M. Pallot, B. Trousse, M. Nilsson, and A. Oliveira, "Smart cities and the future internet: Towards cooperation frameworks for open innovation", in The future internet assembly, Springer, Berlin, Heidelberg, 2011, pp. 431-446.
[5] M. Janssen, S. A. Chun, and J. R. Gil-Garcia, "Building the next generation of digital government infrastructures", Government Information Quarterly, Vol. 26, No. 2, 2009, pp. 233-237.
[6] A. Ojo, and J. Millard, Eds., "Government 3.0–Next Generation Government Technology Infrastructure and Services: Roadmaps, Enabling Technologies & Challenges", Springer, Berlin, 2017.
[7] D. Boos, H. Guenter, G. Grote, and K. Kinder, "Controllable accountabilities: The Internet of Things and its challenges for organisations", Behaviour & Information Technology, Vol. 32, No. 5, 2013, pp. 449-467.
[8] U. H. Westergren, T. Saarikko, and T. Blomquist, "Initiating the Internet of Things: Early Adopters' Expectations for Changing Business Practices and Implications for Working Life", in The Internet of People, Things and Services, C. Simmers and M. Anandarajan, Eds., Routledge, London, 2018, pp. 111-131.
[9] European Parliament, Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data", April, 2016.
[10] G. Valdés, M. Solar, H. Astudillo, M. Iribarren, G. Concha, and M. Visconti, "Conception, development and implementation of an e-Government maturity model in public agencies", Government Information Quarterly, Vol. 28, No. 2, 2011, pp. 176-187.
[11] A. Schumacher, S. Erol and W. Sihn, "A maturity model for assessing industry 4.0 readiness and maturity of manufacturing enterprises", Procedia CIRP, Vol. 52, 2016, pp. 161-166.
[12] J. Luftman, "Assessing Business-IT Alignment Maturity", Communications of the Association for Information Systems, Vol. 4, No. 1, 2000, paper 14.
[13] United Nations & American Society for Public Administration (ASPA), Benchmarking e-Government: A Global Perspective. United Nations, New York, 2002.
[14] A. Grönlund, "Ten years of e-government: The 'end of history' and a new beginning", Electronic Government, Lecture Notes in Computer Science, Vol. 6228, 2010, pp. 13-24.
[15] L. Atzori, L, A. Iera, and G. Morabito, "The Internet of Things: A survey", Computer Networks, Vol. 54, No. 15, 2010, pp. 2787-2805.
[16] D. Miorandi, S. Sicari, F. de Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges", Ad Hoc Networks, Vol. 10, No. 7, 2012, pp. 1497-1516.
[17] J. Kallinikos, A. Aaltonen, and A. Marton, "The Ambivalent Ontology of Digital Artifacts", MIS Quarterly, Vol. 37, No. 2, 2013, pp. 357-370.
[18] E. Borgia, "The Internet of Things vision: Key features, applications and open issues", Computer Communications, Vol. 54, 2014, pp. 1-31.
[19] A. Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things—A survey of topics and trends", Information Systems Frontiers, Vol. 17, No. 2, 2015, pp. 261-274.
[20] N. V. Wünderlich, K. Heinonen, A. L. Ostrom, L. Patricio, R. Sousa, C. Voss, and J. G. Lemmink, ""Futurizing" smart service: implications for service researchers and managers", Journal of Services Marketing, Vol. 29, No. 6/7, 2015, pp. 442-447.
[21] P. P. Ray, "A survey of IoT cloud platforms", Future Computing and Informatics Journal, Vol. 1 No. 1-2, 2016, pp. 35-46.
[22] F. Wortmann, and K. Flüchter, "Internet of Things", Business & Information Systems Engineering, Vol. 57, No. 3, 2015, pp. 221-224.
[23] I. Lee, and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises", Business Horizons, Vol. 58, No. 4, pp. 421-440.
[24] C. E. Catlett, P. H. Beckman, R. Sankaran, and K. K. Galvin, "Array of things: a scientific research instrument in the public way", in Proceedings of the 2nd International Workshop on Science of Smart City Operations and Platforms Engineering, ACM, 2017, pp. 26-33.
[25] LoRa Alliance, "A technical overview of LoRa® and LoRaWAN™", Retreived from https://lora-alliance.org/sites/default/files/2018-04/what-is-lorawan.pdf, November, 2015.
[26] T. Saarikko, U. H. Westergren, and T. Blomquist, "The Internet of Things: Are you ready for what's coming?", Business Horizons, Vol. 60, No. 5, 2017, pp. 667-676.
[27] G. Walsham, "Interpretive case studies in IS research: nature and method", European Journal of Information Systems, Vol. 4, No. 2, 1995, pp. 74-81.
[28] H. K. Klein, and M. D. Myers, "A set of principles for conducting and evaluating interpretive field studies in information systems", MIS Quarterly, Vol. 23, No. 1, 1999, pp. 67-93.
[29] R.K. Yin, Qualitative research from start to finish. Guilford Press, New York, 2011.
[30] B. Chakravorti, A. Bhalla, and R. S. Chaturvedi, "Countries' Digital Competitiveness, Indexed", Harvard Business Review. Retrieved from https://hbr.org/2017/07/60-countries-digital-competitiveness-indexed. July 12th, 2017.