Myndigheten för samhällsskydd och beredskap

GÖTEBORGS UNIVERSITET

STUDY

Internet of Things: Threats and Opportunities for Society

Facts

This report aims to provide an overview of current developments related to the Internet of Things (IoT) in Sweden and in Swedish government agencies. The report outlines the current definitions of this term, the frameworks of related research, and the findings from the empirical research. Our analysis is intended to be used as a baseline to direct future research funding.

February 2018

Juho Lindman and Ted Saarikko, Applied IT, University of Gothenburg

MSB contact person:
Carina Olsson, 010-240 41 71

Publication number MSB1194 – April 2018
ISBN 978-91-7383-817-7

MSB has ordered and financed this research effort. The researchers are solely responsible for the report's content.

Foreword

Digitalization in general, and the Internet of Things (IoT) in particular, are dramatically transforming societies. Organizations consider promising and novel connected technologies, devices, and practices; their pros and cons are evaluated, and consequently they are taken into use. Traditional "things," for example cars, tunnels, and wheelchairs are increasingly connected to the Internet and other networks. New business models emerge and traditional institutions transform, which impacts both the industries and the public sector.

These developments also raise a number of questions related to accidental and intentional threats as well as mechanisms that societies can take into use to mitigate these threats. Threats range from security of the actual physical devices to risks to entire firms and sectors of the economy, if the connected devices' networks are hijacked and used as botnet to overload other systems. New and old questions of connectivity, privacy, data capture, and security are raised when designing these devices and systems that rely on connectivity.

Governmental agencies play a key role in how successful and widespread IoT-technologies are in different industry sectors. Usually these technologies are not developed in a siloed manner: development takes place in ecosystems, clusters, and sectors where a number of different actors combine their efforts for success. Some of these actors are likely from the public sector, and some are from the private sector.

This leads to a number of governance challenges and tensions, for example whether IoT-based solutions are perceived as national infrastructure or commercially-owned platforms or both, and unanswered questions emerge about data ownership and interoperable standards of the devices, data, applications, networks, and systems.

In what follows, we address these issues by providing an account of state-of-the art research, definitions, and framework from scientific journals. This effort is combined with an empirical investigation using key-person interviews from Swedish agencies. The findings raise a number of observations related to current status of IoT in Sweden, the role of agencies—and MSB—in advancing IoT that need to be further investigated in future research.

Lindholmen, Gothenburg, 23. Feb., 2018

Juho Lindman and Ted Saarikko

Contents

Sammanfattning på svenska

Digitalisering i allmänhet och Sakernas Internet (eng. Internet of Things, IoT) i synnerhet för med sig dramatiska förändringar för samhället. Såväl företag som offentliga verksamheter ser många fördelar med att anamma ny teknik i sina interna processer och externa produkter och tjänster.

Statliga myndigheter spelar en nyckelroll för att främja framgångsrik diffusion av IoT-teknologier inom olika sektorer av industri och samhälle. Baserat på vårt teoretiska och empiriska arbete föreslår denna översiktsrapport ett antal konkreta åtgärder för att främja säker utveckling av IoT i Sverige.

Denna översikt detaljstuderar inte detaljerna i enskilda sektorer och den teknik som tillämpas, men belyser områden där framtida forskningsfinansiering bör främja studier av sektorspecifika aktiviteter, strategier och aktör. Framtida forskning bör ta hänsyn till både sociala och tekniska problem i samband med omfattande tillämpning av IoT.

Ytterligare forskningsinsatser behövs också i samband med sektorsövergripande och systemiska utmaningar. Trots att skillnader existerar mellan olika delar av samhället är tekniska funktioner och organisationslogik ofta snarlik vilket gör att privata och offentliga aktörer ofta står inför liknande problematik och kan vinna på att samsas kring gemensamma tekniska plattformar och infrastrukturer. Man har dock en tradition av att lösa problem på olika sätt vilket måste beaktas i relationen mellan privat och offentlig sektor.

Den fråga som alltjämt dominerar diskussionen kring digitalisering och IoT är säkerhet. Uppkopplade enheter innebär nya säkerhetshot och angreppssätt för anslutna system. Konsekvenser när kritiska system angrips kan vara förödande. Nya förmågor måste utvecklas för att mildra både avsiktliga oavsiktliga hot mot samhället.

Vårt arbete ger upphov till flera frågor om hur IoT skulle kunna regleras och mer specifikt hur den regleringen skulle kunna organiseras. Övriga identifierade möjligheter till forskningsfinansiering berör **pågående digitalisering**, **styrning av ekosystem med privata och offentliga aktörer**, samt **inneboende tekniska risker med uppkopplade enheter**. Det finns ett behov av både teoretiskt arbete och tillämpad forskning, till exempel med hjälp av praktiska implementationer av tekniska lösningar.

Det internationella sammanhanget är av stor betydelse inom detta område eftersom den tekniska utvecklingen sker globalt. Forskningsinsatser bör dra nytta av de senaste framsteg som rapporterats i internationella publikationer och toppmoderna tekniska tidskrifter. Då våra grannländer står inför liknande utmaningar är det relevant att jämföra problemställningar och lösningar. Forskningsinsatser skulle kunna utvidgas till att jämföra den offentliga sektorns tillvägagångssätt för IoT i bl.a. Finland, Estland och Norge.

Executive summary

Based on our theoretical and empirical research, this overview report suggests a number of concrete actions to safely and efficiently advance IoT in Sweden.

This overview does not delve deeply into the details of the individual sectors and the technologies implemented in them, although future research needs to investigate detailed sector-specific activities, strategies, and actors. Research focus should take into account both social and technical issues related to the ramp-up of IoT-technologies.

Further research efforts are also needed related to cross-sectoral and systemic challenges. Even though sectoral differences exist, technical functionalities and organizing logics are similar, thus private and public stakeholders face similar challenges across sectors.

This report identifies a number of governance challenges related to the complex ecosystem interplay of public and private actors. Conflicting institutional logics and objectives need to be managed. Ecosystem and platform competition–related issues emerge. Openness of the platforms and infrastructures is one aspect to take into account.

Security issues are increasingly taken more seriously. New connectivity offers novel security threats and attack vectors to connected systems. Consequences from critical systems failures can be devastating. New capabilities need to be developed to mitigate both the accidental and intentional threats to society.

Our work raises several questions relating how IoT could be regulated and, more specifically, how that regulation could be organized. Other funding opportunities identified are related to **continuous digitalization**, **multi-stakeholder ecosystem governance,** and **inherent technology risks**. There is a need for both theoretical work and applied research, for example using design experiments.

The international context is of great importance in this area because technological development happens globally. Research efforts in this area should draw on recent advances reported in international publications and state-of-the art technology reviews. Other neighboring countries are facing similar challenges, so comparing and investigating relevant benchmarks would likely provide valuable insights. Research could be extended, for example, by comparing public sector approaches to IoT with Finland, Estonia, and Norway.

1. Introduction

1.1 Research task

Increased connectivity and hardware developments such as sensor technology and distributed computing are leading to dramatic changes in society, as digital and physical systems are being designed as increasingly dependent on each other. The aim of this transformation is to enable connected objects to be sensed and controlled remotely over a network, as doing so will provide users with further functionalities and services.

Everyday objects such as cameras, cars and dishwashers are increasingly becoming connected, leading to a network of devices called the Internet of Things (IoT). This term was first used in reference to communication among a global network of things around 2000 at the Massachusetts Institute of Technology Auto-ID Center, which was developing radio-frequency identification (RFID) technology. The idea then was to gather information on each tagged object from an internet/database entry called an Electronic Product Code (a universal identifier). Today, the concept of things includes many kinds of objects and is not only limited to RFID devices. Developed identifiers make things easily readable, recognizable, locatable and controllable via internet connectivity. This connectivity also offers users the ability to activate the devices' functions. Things have also become "smart" – meaning that they have the ability to sense, compute and communicate with their environment and each other.

The transition to the IoT provides huge value potential according to for example Gartner (2015), McKinsey (Manyika et al., 2013) and the Economist Intelligence Unit (2013). However, although it accelerates the economy and provides new high-value services, increased connectivity also poses a number of challenges, including unforeseen security risks that need to be mitigated. Some of these risks are related to specific new equipment, but the more systemic risks are related to increased connectivity and the dependencies between large-scale physical and digital systems.

In addition to device manufacturers and commercial service providers, the public-sector agencies that are responsible for providing the infrastructural backbone of this network may play a key role in identifying and mitigating future problems. Therefore, we first provide a scientific overview of the phenomenon and of the current focus of such Swedish agencies, including their initiatives, organization and capabilities in this rapidly changing area.

1.2 Research implementation

Our report aims to provide a baseline that can be used in analyzing the current situation, revealing interesting opportunities or challenges and directing future

research funding. We include a literature review that discusses the key definitions, the main theories and the scientific state of the art regarding the IoT.

Then, we proceed to an empirical study consisting of key-informant interviews with Swedish experts from public agencies working in the IoT area. Our focus is at the societal level: we try to limit introducing technical detail of the devices or connectivity only to highlight some of the tasks at hand.

Our research question is as follows: What is the IoT (perspectives and definitions), and more specifically, what are the security issues, threats and risks related to the IoT at the societal level? Our analysis focuses on how public agencies currently work with and organize for the IoT, including their views of how knowledge, capabilities and resources are developing in their sectors.

The answers to these questions help establish a general baseline that can be used to direct future research funding in Sweden, both in specific sectors and across sectors.

The report is structured as follows: First, we provide an overview of the phenomenon, and then we discuss the sources we used and the research literature on the topic. This is followed by a discussion of our empirical work; we report our results and provide analyses, discussion and recommendations based on both the theoretical and the empirical work.

2. Internet of Things as a phenomenon

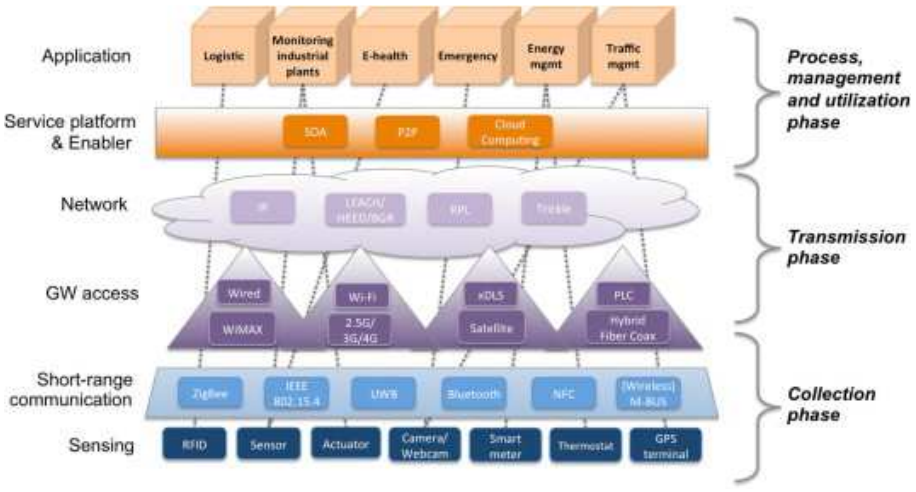
2.1 Toward a connected society

The IoT is a highly emergent field in research and practice. It is difficult to find absolute and precise definitions of what constitutes the IoT. Moreover, it is impossible to limit the IoT to any specific technology. For instance, RFID technology is often associated with the IoT, as it permits users to assign a digital identity to a physical object (e.g., for the purposes of logistics). However, that does not mean that every application of RFID is part of the IoT. Rather, the IoT is largely defined by the manner in which devices are connected, thus permitting data to be shared, combined and used.

Hence, although technical infrastructure enables the IoT, its formation is ultimately a multifaceted process in which technical standards, business incentives and legal frameworks come together to form a complex socio-technical system.

Although the main purpose of this report is not to describe all the relevant technologies involved in implementing the IoT at the societal level, it is necessary to discuss the IoT's technical design space to get a better understanding of its potential risks and benefits.

Borgia (2014) provides a non-exhaustive overview of some of the key technologies (see Picture1). Additionally, the list is vertical; the idea is to get out of the traditional (horizontal), proprietary siloed infrastructure, which relies on proprietary solutions and devices, leading to unnecessary redundancy and added costs (Borgia, 2014). Instead, a common operational platform could be used to manage the network and provide the services (see Picture1).



Picture1: Vertical list of IoT technologies and protocols

Picture1 shows the technologies related to sensors and RFID, and it is divided into three distinct phases: 1. Collection, 2. Transmission and 3. Processing. In the Collection phase, the physical objects are identified, or their parameters are sensed. Technologies such as IEEE 802.15.4 and Bluetooth are used to collect the data. In the Transmission phase, the data are moved via gateways and other infrastructure to servers, where computational operations are performed.

The related technologies include networks (e.g., wired, wireless and satellite) and routing (e.g., LEACH, RPL and Trickle). The third phase, Processing, involves handling the data flows and managing the processes – for example, identifying and managing the devices or aggregating and semantically analyzing the data. These various technologies (and their acronyms) are listed in a separate table (see Appendix1).

2.2 IoT service platforms

Platforms are one of the layers in the suggested IoT ecosystem. Earlier researchers have discussed several types of platforms, drawing on various scientific theories: organizational platforms, product-family platforms, market-intermediary platforms and platform ecosystems (Thomas et al., 2015).

Two key concepts underlie these types of platforms: 1) leverage, in which companies exercise influence disproportionate to their size so as to produce greater outputs (often value), and 2) architectural openness, which enables various actor configurations. For private companies, these dynamics also offer opportunities for novel and emerging business models related to IoT (Dijkman et al., 2015).

In general, the digital-platforms research has focused on how various platforms enable global resource sharing and task organization (de Reuver et al., 2017). On these platforms, capital, labor, goods and information can be exchanged in peer-to-peer fashion. Platforms can also be used to coordinate offline commercial activities such as housing, dining and transportation in the so-called sharing economy.

Borgia (2014) describes in detail how IoT service platforms operate; they belong to phase 3 (Processing) and involve managing and utilizing information flows, processing them and forwarding them to other applications. This requires that the technical architecture's details (hardware, software, data formats, etc.) and heterogeneity be hidden to decouple the applications from the underlying components. Mechanisms such as SOA, peer-to-peer and cloud-based approaches can be used to accomplish this aim.

Innovation related to digital objects often relies on a layered approach (Yoo et al., 2010). This separation into layers can be done using boundary objects and resources (Yoo et al., 2010), thus decoupling business assets and application software to enable digital innovation. This decoupling can also be

complemented with open innovation activity that is orchestrated across company boundaries, resulting in third-party contributions and *generativity*, which, in this context (Tilson et al., 2010), refers to a technology platform's or ecosystem's ability to "create, generate or produce new output, structure or behavior without input from the originator of the system."

The paradox of generativity is a theoretical tool used to discuss the research tension between infrastructural control logic and generativity (Eaton et al., 2015). Infrastructural control research aims to exercise control through the use of standards that manage access to the service system (Lyytinen & King, 2006). To solve the tension between infrastructural control and generativity, boundary resources (for example, application programming interfaces) can be used; these include the rules for the interface between platform owners and application developers (Ghazawneh & Henfridsson, 2013).

Choosing an optimal level of openness for a platform is a critical decision taken by the platform owner. On one hand, opening intellectual property of the platform may offer increased generativity by increasing innovation spillovers from third-party developers and increased revenue for the complementary products and services. On the other hand, opening up the ecosystem up will mean losing direct revenue and "risk" increased competition (for more on this choice, see, for example, Parker and Van Alstyne, 2017).

Christensen et al. (2015), for example, have worked extensively on disruption, the business dynamics of how smaller entrants challenge dominant players by targeting overlooked segments and by providing new functionalities (often with a lower price). When entrants have secured their position, they move to the mainstream, reconfiguring the industry landscape and competitive position of the companies. Disruption has taken place when incumbent companies start to adopt entrant business strategies. Another relevant stream of literature on industry transformation focuses on changes in the institutional frameworks of organizational fields (industries). Institutions mean regulative, normative, and cognitive structures and activities that provide stability and meaning to social behavior (Scott, 2014). Thus, formal and informal rules of the organizational field are the focus rather than supply and demand on the marketplace.

Traditionally, competition is seen among "pipeline" businesses that aim to optimize their activities in the value chain (linear series of activities) under the direct control of companies. Currently, literature raises the prospect of increased interest toward platform companies (Van Alstyne et al., 2016) where a key asset is a user or developer community that lies outside the direct control of the company. This leads to competitive situation shifts whereupon important actors orchestrate activities, not directly control resources. Industries move from optimizing internal processes to creating positive network effects that increase the economic value of the whole ecosystem. Platforms compete against platforms, companies compete against other companies, and companies may compete against other platforms. In the pipeline business, key strategical components revolve around erecting barriers. Platform competition, however, relies more on orchestrating the different resources in the ecosystem, whether private or public).

IoT service platforms often contain larger, heterogeneous actors; thus, governing them is even more difficult than for some of the more traditional platforms. These service systems require different capabilities and have stakeholders who need to be brought together, limiting the governance options for platform owners. Many earlier works on the competition between platforms and standards seem quite applicable to the IoT domain as well.

2.3 Ecosystem risks

Reverse network effects are one of the main threats of widespread IoT connectivity (Atzori et al., 2010); for instance, coordinated DDoS (Distributed Denial of Service) threats could be realized via access to poorly secured devices, leading to widespread use of IoT networks as botnets.

Security concerns can be divided into four distinct challenges, some or all of which need to be overcome for a given application: 1) secure authentication or authorization, 2) secure object bootstrapping and data transmission, 3) secure data and content, and 4) secure access (by people).

Several characteristics make IoT services especially vulnerable. 1) They are usually unsupervised, so it is easy to get physical access to them; 2) unless it is encrypted, wireless communication can pose challenges in terms of monitoring traffic; and 3) low computing and energy-consumption capabilities (as well as cheap prices) may lead to security compromises. Specifically, device authentication and data integrity are areas of concern. Things must be what they say they are (Whitmore et al., 2015).

Privacy and (especially) consent in data ownership are other issues that emerge when increasing the number of trackable objects. Users also need to be able to trust the IoT if they are to accept it. Thus, issues related to data ownership and privacy policies need to be managed.

Novel legal challenges are also likely to emerge (for example, issues related to the governance of novel assets and data). Various shared governance structures are needed to manage this complex ecosystem (Whitmore et al., 2015).

Both public- and private-sector activities are likely needed regarding the IoT and its impacts so as to mitigate the outlined risks. However, researchers will need to delve deeper into industries and sectors to better understand the current situation (including the capabilities that need to be developed) and to discuss future needs regarding the governance of these ecosystems.

2.4 Digitized products and digitalized processes

Connected products are among the most commonly cited examples of the IoT and of the changes that follow in its wake. Products that are imbued with new capabilities may either serve a broader range of uses or, via complicated learning algorithms, anticipate users' needs (rather than remain passive).

Porter and Heppelmann capture the gist of these developments: “Once composed solely of mechanical and electrical parts, products have become complex systems that combine hardware, sensors, data storage, microprocessors, software, and connectivity in myriad ways” (2014, p. 66).

Two distinct phenomena drive the development of connected products: digitization and digitalization (Tilson et al., 2010). The former, digitization, refers to the addition of digital components or capabilities to physical products. Through digitization, a product may retain its traditional properties while also gaining additional functionality such as reprogrammability, which makes it possible for the product to be modified after it has left the factory. Coupled with remote connectivity, such modifications can even be delivered at a low cost and without transporting the product to a dedicated location (e.g., a repair shop or a service station). The ability to access and/or modify products after delivery enables both new product features and new business models. In terms of features, a supplier can continually monitor a connected product. This, in turn, offers the possibility of optimizing the product during its life span by matching its internal settings to the manner in which it is actually used. Moreover, continuous access to a product permits the adoption of predictive (rather than reactive) maintenance. This refers to the ability to conduct maintenance before a product fails rather than only performing repairs after it has already broken down.

Digitalization, on the other hand, refers to the manner in which digitized products affect existing business models and organizational processes. For instance, the aforementioned predictive maintenance permits service and maintenance to be performed when it is causes the least disruption to related organizational processes. Remote access to smart products can also have a more profound impact in that it facilitates *servitization* – a shift from product retail to service provision (Oliva & Kallenberg, 2003). In a servitized business model, the manufacturer still provides a product to the customer; however, rather than receiving a one-time payment in an ownership exchange, the manufacturer retains ownership of the product, and the customer pays a fixed monthly fee for its use. This arrangement is hardly a novelty as the concept of *leasing* rather than purchasing a product has been around for many years. Connected products are however poised to widen the scope and appeal of servitization as they enable more responsive service (for customers) and fewer service-related risks and costs (for manufacturers).

2.5 Societal impact across multiple sectors

In the past few years, the IoT has attracted increasing interest in both the private and public sectors. Borgia (2014) outlines three broad domains of application: *smart cities* (e.g., public transportation, electrical grids, buildings and emergency services), *health and well-being* (e.g., e-health and independent living), and *industry* (e.g., industrial manufacturing, agriculture and logistics).

Each domain can be broken down in several ways into multiple niches that describe specific situations, stakeholders and purposes for which the judicious

use of technology could create greater automation of menial tasks, better-informed operational and managerial staff, or even fully revamped and transformed organizational processes. In what follows, we will briefly outline some concrete examples of how IoT has been applied in the different sectors.

2.5.1 Smart cities and energy

Companies and other commercial interests are not the only entities intrigued by the IoT. Government agencies and municipalities are keenly interested in the possibility of leveraging connected devices to better serve their citizens as well as conserve energy. However, a 2015 report from Arthur D. Little demonstrates that creating a "smart city" is not easy and only a handful of ventures have made significant progress (Schlautmann et al., 2015).

One of the more ambitious projects is in Chicago, where the city has teamed up with the University of Chicago to equip streetlights with sensors (or *nodes*, as they are also called) that can sense temperature, barometric pressure, light, noise, vibration, carbon monoxide, nitrogen dioxide, sulfur dioxide and ground-level ozone. In the near future, Chicago hopes to further expand these parameters to include air pollution and floodwater – which have been frequent problems in the city for several years. The project is called Array of Things[1], and it aims to provide real-time monitoring of the city as a whole and of its individual districts.

This fine mesh of sensors provides access to information that is specific to a particular street or neighborhood. In this way, Chicago's civil servants and town planners can monitor the city's environment and allocate resources where needed, and researchers can map trends in urban development over time. Furthermore, the resulting data can be published openly and free of charge, enabling the development of applications that benefit residents – for example, by helping people avoid areas with poor air quality or excessive noise and congestion. Furthermore, the city has actively worked to incorporate the project into the curricula of the city's high schools and colleges (e.g., by holding workshops in which students learn to build sensors that provide relevant information in an urban environment). During the initial phase of the project, in the summer of 2016, more than 40 nodes were installed around the city. However, the plan is for the number of nodes to grow to 500 in 2017-2018.

Unlike Chicago, Amsterdam represents a relatively mature venture within the application of IoT in an urban environment. Starting as early as 2009, the city has organized and supported a variety of different initiatives intended to support living in a densely populated urban environment. One of the city's profile areas is development towards a circular economy[2] and seek new ways to reduce, recycle and reuse different resources. Energy is a tangible example where the city is working towards being producers as well as consumers of electricity. By fitting residential houses with solar panels, transformers and

[1] http://arrayofthings.github.io/

[2] https://amsterdamsmartcity.com/circularamsterdam

batteries, the long-term goal is to turn housing areas into virtual power plants that can become self-sufficient or even sell surplus power to the city.[3]

Through their smart city-initiative, Amsterdam also encourages external actors to develop and launch their own solutions that are in line with the city's environmental thinking. For example, with the support of a local incubator for tech-ventures, a “smart” wall connector, Crownstone[4], has been developed that can be linked to several different devices such as your phone or a simple "tag" worn in a key ring. You then program how the wall connector should respond to your presence. A simple application is to automatically switch on the lights as you walk in to a room and turn them off again as you leave.

While may be convenient for the user, the main benefits are reduced energy consumption and added security. Up to 10% of our electricity bill consists of appliances (such as TV, computer, kitchen appliances) which remain in stand-by mode an continuously consume electricity as long as they are connected to the mains power supply. If we were instead to disconnect them from the power supply when we leave the room (or our house) we could feasibly save a great deal of money on a yearly basis with virtually no added effort. The safety aspect is arguably even more important as the same technology can ensure that a piping hot clothes iron is not left unattended or small children accidentally turn on the stove. By encouraging and marketing new, smart technical solutions, the city of Amsterdam hopes to gain support from both citizens as well as the private sector in order to collectively build a greener city.

Another example from the energy sector would be so called smart grids i.e. intelligent electrical systems that deliver energy directly from producers to consumers and in bidirectional way.

2.5.2 Health and well-being

The demographics of most developed countries are undergoing a major shift, as the life expectancy of these countries’ citizens continues to climb into the 70s and 80s. Although a long life expectancy is ultimately a sign of amenable social and economic conditions, it also carries with it the need to deliver health care to a larger number of citizens, which is particularly challenging for countries that have fixed sets of resources. Part of the solution is to shift as much care as possible away from dedicated health care facilities (e.g., hospitals) and to instead enable citizens to live in their own homes, even if they occasionally need assistance.

A 2016-2017 survey of Swedish municipalities[5] indicates that health care is the most common area for public-sector applications of IoT. Connected equipment can provide secure living arrangements by alerting health care personnel if an individual in fact does require help. For instance, specialized cameras can be used to periodically check in on a person during the night to see ensure that he

[3] https://amsterdamsmartcity.com/projects/city-zen-virtual-power-plant

[4] https://amsterdamsmartcity.com/products/crownstone

[5] Results may be viewed at https://iotsverige.se/omvarldsbevakning/

or she is resting comfortably. Another example is pressure pads, which can sense unusual weight distributions, perhaps indicating that a person has collapsed on the floor. Health care services can then immediately be summoned to assess the situation and render aid. Both solutions serve to provide both quantitative and qualitative benefits, as staff resources can be diverted wherever they are most needed, and residents can be sure that they will receive help when needed – regardless of whether they can get to a phone.

Looking to the future, the EU-funded project RemoAge[6] is developing and testing new means to support senior citizens living in northern Scandinavia, Scotland and Northern Ireland. The purpose of the project is to leverage modern digital technologies to provide increased safety and access to healthcare despite living in sparsely populated areas where access to public services is often several hours away. In addition to supporting citizens, the project also strives to better organize and utilize resources in order to better match healthcare requirements with healthcare provision. One such measure is the introduction of *remote professional consultation* whereby the patient converses with healthcare professionals via digital devices such as tablet PCs. Conducting initial consultations and queries remotely conserves healthcare resources and saves citizens traveling long distances to access healthcare. Furthermore, as remote consultations are unrestricted by distance, patients can consult with specialists that reside even further away than their closest healthcare facility.

The ability to provide continuous access to healthcare is especially important for elderly citizens who are more likely to suffer from chronic conditions such as diabetes or high blood pressure. With the aid of modern medical devices, citizens are often able to monitor their own condition and then consult with healthcare personnel.

2.5.3 Industry and transport

The industrial domain stands to gain significant advantages by adopting IoT into their processes. Equipping heavy machinery with sensors can serve to quantify *operational status* and efficiency, providing valuable information regarding if and when service is necessary. Complementing sensors with remote connectivity provides access to this information irrespective of location, making gathering and aggregation of data an entirely automated process. From that point, it is merely a matter of applying the correct algorithms to sort through the data and finding the useful information hidden within. For instance, insights into the wear-and-tear of different components or knowing which product features customers appreciate could provide invaluable input to future product development. Moreover, data streams from different machinery can be integrated in an effort to supervise an otherwise heterogeneous manufacturing process consisting of several distinct steps. IT-supported

[6] http://remoage.eu/

supervision and analysis of industrial processes has produced its own stream of research commonly associated with the term industry 4.0 (Lee et al., 2015).

In addition to supervising the status of products – or production processes – IoT has been widely applied to determine the *location* of objects. Indeed, the origin of the term Internet of Things is commonly attributed (Ashton, 2009) to logistics where increasingly long and winding supply routes struggled under the burden of manual information management. By furnishing shipments with RFID-tags, physical objects could be supplemented with a digital counterpart, creating a tight coupling between the actual location of the physical object and designated location given in a computerized system.

Both aspects – operational status and location – converge in the application of IoT to remote supervision and/or control of vehicles for personal of commercial use. While the prospect of self-driving cars has attracted a lot of news coverage recently[7], connected vehicles as such are essentially old news. One of the more eye-catching examples is Tesla, which periodically updates the software in its cars to improve performance or add new features. Although connected personal automobiles offer a tantalizing glimpse at where the automotive industry is heading, the advent of internet connectivity is arguably more significant for other types of vehicles.

Buses and trucks are commercial vehicles, and they have to remain in virtually constant use during the workday to warrant their costs. They are also rather large vehicles, and they consume a considerable amount of energy, leaving a significant carbon footprint. As such, adding internet connectivity to these vehicles offers several opportunities that are focused on utility and tangible benefits, unlike the user-centric features of personal automobiles.

First and foremost, connected vehicles can use IT-supported, fuel-efficient driving, or *ecodriving*. This requires only a relatively basic technical infrastructure, which can be retrofitted to older vehicles as well – software that analyzes driver behavior and provides feedback to encourage a driving style that reduces fuel consumption. Such recommendations include greater caution when starting and stopping as well as optimum driving speeds. Ecodriving is ultimately focused on driver attitude and behavior, and IoT-based tools can help inform drivers about the effects of certain actions, such as by having an interface blink red when fuel is being wasted but blink green when fuel is being saved. Evidence from logistics and public transportation suggests that ecodriving can reduce fuel costs – and resulting air pollution – by as much as 10%.

In addition, a connected vehicle can also be tracked more reliably (e.g., using GPS technology). Again, this is by no means a novelty, as GPS navigation has been around for many years. However, a reliable means for tracking the whereabouts of commercial vehicles also provides an opportunity for *geofencing* – the ability to map the actual a vehicle's position to a predetermined set of permissible routes and locations. Interest in geofencing

[7] https://www.svt.se/nyheter/vetenskap/forskare-sjalvkorande-bilar-forandrar-staderna-inom-bara-nagra-ar

has recently been reignited due to incidents in which trucks have been stolen and used to indiscriminately target people in urban areas[8]. The goal is to detect erratic behavior before a would-be perpetrator has the chance to cause any serious harm. Other potential uses of geofencing include supervision of the transportation of hazardous materials to prevent deviation from the intended route.

2.5.4 Other areas: Food, financial services, information and communication and security

It is possible to divide the sectors and agencies in different ways (Borgia et al., 2014), but, traditionally, most of the research has fallen under the described three categories: smart cities and energy, health, and industry and logistics). For the purposes of this report, we have used the division of seven sectors and, thus, list some emerging research and pilot programs that do not fall directly under the mentioned three from the four other sectors of food, financial services, information and communication, and security.

Food. Many of the benefits described for the production and transportation of food also apply to the industry and agencies dealing with the production and distribution of foodstuffs in society. The supply chain, delivery networks, and regulation environment regarding foodstuffs are all relatively complex (Pang et al., 2015). This leads to challenges in guaranteeing public food safety and quality. IoT has been suggested as a solution due to the distributed nature and geographical scale of the challenges, for example by offering better traceability, visibility, and controllability challenges (Xu et al., 2014).

An example application from the food-IoT area is Food Supply Chain (FSC) solutions. Normally, FSC consists of three key parts: field devices that are used to tag the goods at the origin, backbone systems for storing the data, and the distributed communication infrastructure to support tracking of goods. The primary function of these systems is to track the origin and monitor the process of food production through the whole chain, for example tracking the RFID all the way from the producer to the intermediaries to the consumer. A more specific example of IoT relates to agricultural animals (Borgia et al., 2014), where authorities normally require full traceability and continuous monitoring of the animals. Advanced IoT services may also be used for registering and monitoring of farms and the issuance of health authorizations.

Financial services. IoT is used in different industries that involve financial transactions between companies, individuals, and organizations. Financial services may use IoT approaches in a number of ways, where the primary objective is to increase the data used in making decisions. For example, to increase the accuracy of underwriting car insurance policies, companies could collect data to determine car mileage, assess driver performance, and map vehicle location.

[8] https://computersweden.idg.se/2.2683/1.683009/geofencing

We have seen pilots and development efforts in this area, for example Groceries by Mastercard, which links the provided Mastercard with a Samsung refrigerator[9]. Another example is Visa's Mobile Location Confirmation, which aims to identify credit card fraud by using app and mobile phone location data.

Information and communication This sector usually handles efforts related to regulation and standardization in both national and international contexts. Often authorities in this sector play key roles related to the provision and maintenance of infrastructure required by the IoT, for example Internet connectivity, landline telephones, and mobile telephone networks.

A key international organization is International Telecommunications Union (ITU), which has been pushing for IoT global technical standards in the area titled SG20[10].

Security. One of the key tasks of local and national governments is to provide security to societies by maintaining public safety (public order, protection of individuals, etc.) and emergency management (natural and non-natural disasters). IoT can be used to monitor and tackle these scenarios (Dong et al., 2017). Surveillance cameras can be used for a number of purposes, for example to maintain public order. Sensor technology can be installed to improve safety in different ways.

Example application areas include improved firefighting capabilities through better real-time location and tracking data that can be used to provide a detailed map of the event. IoT devices, such as personnel card information or existing cameras of the building, might also be useful in firefighting operations, for example to identify the number of people in a building.

[9] https://newsroom.mastercard.com/press-releases/mastercard-samsung-make-everyday-shopping-easier-in-tomorrows-smart-home-with-launch-of-groceries-by-mastercard-app/

[10] https://www.itu.int/en/ITU-T/studygroups/2017-2020/20/Pages/default.aspx

3. Sources and research boundaries

3.1 Research statement

The potential scope of the related works is huge and could span several sciences (both social and natural). The phenomenon's technical complexity and unclear borders result in a situation in which a number of limitations are required.

Therefore, we focused on leading journals and on established articles that indicate a solid direction of the research. In this work, we have primarily used the lens of information systems (informatics) and have also drawn on the more technical engineering sciences. Using information systems lets us discuss digital and physical artifacts as ***socio-technical systems***, where focus is on the interactions between people and technology (in business settings) (Lee, 2001).

We approach these artifacts in a social context, and our research challenges are related to their societal design and impact. This approach also enables us to draw on rich methodological literature regarding how these artifacts change societies and social institutions – more precisely, focusing on necessary governance capabilities and on the public sector's role in emerging IoT ecosystems.

3.2 Scope and limitations

We focus on highly cited outlets, drawing on papers, reports and expert opinions to provide rich context for this study. The IoT is an emerging field of research in several competing scientific fields and projects; it is also an emerging societal transformation.

Research on the IoT has focused on the societal, group and individual levels. In this work, we mainly focus on the societal level. Additionally, much of the work that is focused on IoT artifacts' functionalities, characteristics, affordances, designs and uses could be relevant to this study. For example, risk, security and privacy are distinct research fields and subfields with established research communities, traditions, methodologies and outlets.

Expertise from several kinds of backgrounds is needed to make IoT initiatives successful due to the complexity and interconnectedness of the technology.

Our focus in the literature review is on impactful research papers that have been published in recent years in high-caliber publication outlets. We primarily focus on the field of information systems, but we also draw on certain more technical papers from other fields. We continue this discussion on the relevant research traditions and definitions in Section 4, and we describe our empirical

work (which also draws on information systems methodology) in more detail in Section 5.

4. Internet of Things as an area of research

In this chapter, we summarize Internet of Things (IoT) as an area of research and provide an overview of relevant concepts. In the interest of clarity, we divide the latter into concepts that are central to understanding IoT and those that relate to different potential applications of connected devices.

4.1 Characteristics of extant research

Practitioners as well as academics quite often refer to IoT as though it represents a single, cohesive body of knowledge. That is however hardly the case. Indeed, some of the most frequently cited works that explicitly refer to IoT do not consider it a homogeneous field of research or practice at all, but rather a heterogeneous collection of different technologies that can be used to link a wide range of different artefacts, e.g. networks, products, components and small tags (Atzori et al. 2010; Gubbi et al., 2013). The technical perspective on IoT is aptly summarized by Miorandi et al. (2012, 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*."

Hence, it is more apt to consider IoT not as a technology, infrastructure or standard, but rather as a design perspective or 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 breakdowns (Wünderlich et al., 2015). The ostensible novelty – and increased attention – associated with IoT does not stem from the development of any single technical innovation or sudden realization that connected products offer new affordances, but rather 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 different locations have plummeted as both wired and wireless networks grow ever more available. By using customized software (called *middle-ware*), we can link different types of networks and machinery and thus provide seamless connectivity despite an increasingly diverse range of devices and applications (Bandyopadhyay et al., 2011; Lee & Lee, 2015; Saarikko et al., 2017).

As the underlying technologies have matured, IoT is no longer limited to a select few areas of application, but stands on the verge of disseminating into every aspect of our society. This is reflected in extant research in which IoT is to varying degrees intertwined with it domain of application (Borgia, 2014). In other words, the application of IoT is not driven by a technical discourse, but rather by advantages sought or problems alleviated. As IoT is starting to have a palpable impact on society – as well as different research communities – it is increasingly driven by different phenomena and scattered across scientific disciplines and publishing outlets. While there are those who have reviewed the topic based on their own academic field (e.g. Lu et al., 2018; Ng & Wakenshaw, 2017; Sou et al., 2012) or reviewed specific areas of application (e.g. Da Xu et al., 2014; Stojkoska & Trivodaliev, 2017; Zanella et al., 2014) there are few general reviews. (See Whitmore et al., 2015 for a notable exception.)

As IoT is approached more as a loosely defined perspective or phenomenon, it naturally follows that academic expertise on the topic is often divided with regards to the relative importance of certain key concepts. Furthermore, different research domains are imbued with their own traditions and standards pertaining to research philosophy and permissible methodologies. As such, it is exceedingly difficult to form a coherent review of the relevant research and to collect key insights from such a review as there is very little common ground on which to base a "definitive" list of results. As such, while we have sought to be neutral in our own appraisal of extant research, it is only natural that this report is shaped by our own background in Information Systems Research. We list the main domains of IoT research in Section 2 and describe our research task in Section 3.

Furthermore, as the IoT is causing a large-scale transformation that impacts industry, society and healthcare, there is a wealth of material beyond just academic reports, including vendor white papers, consultant reports and government guidelines. Moreover, there are ongoing research projects all over the world that seek to further our understanding of IoT as well as refine the underlying technologies. We list a few of the key non-academic sources in the reference list and discuss related Swedish research initiatives and reports in Section 5.5.

Some of the more technical research reports are focused on the devices' design and on their interactions rather than on the user or service sides of the technology or on the societal impacts. There is thus a need for more theoretical work in the area as well as for carefully crafted case studies on the IoT's process, design and usage aspects. Lastly, and perhaps most importantly, we see a need for more empirical work that addresses the long-term societal implications as our ambitions gradually mature from developing and implementing individual solutions and initiatives to comprehensive connected environments that cover entire cities or hospitals or industrial value-chains.

4.2 Central concepts

We list some of the central concepts of the area and their relation to the IoT in Table 1.

Term	Meaning	Relation to IoT
Digitization (Sv. *Digifiering/digisering*)	Process of converting analogue information to digital format (to bits)	This conversion of information is usually part of IoT initiatives.
Digitalization (Sv. *Digitalisering*)	Large-scale societal transformation in which institutions, industries and social relations become reorganized around digital technology	The IoT is one part of this larger transformation of societies and industries
Cyber-Physical Systems	A mechanism that incorporates both physical and digital components and is controlled (or monitored) by algorithms via the internet	This term is sometimes used synonymously with the IoT.
Digital Service Platforms	Computer-based and internet-connected provision of service – usually involving the separation of the platform layer from the applications that run on top of it	The standards and interfaces required to leverage the IoT ecosystem can often be usefully described by breaking them into decoupled layers.

Table1: Central concepts

4.3 Related concepts

We list some of the related concepts that are often used when discussing IoT and short summary of how they are often used in Table 2.

Term	Meaning	Relation to IoT
Big Data	Data sets that are so big and complex that	IoT approaches almost always provide large

	traditional applications can't deal with them	amounts of data for analysis.
Small data	Information that humans can understand and act on	Big data analytics usually includes turning big data into small data.
Algorithmic decision-making	Algorithms that make decisions and devices that perceive their environment and take actions to reach a goal	Some IoT approaches aim to make devices that can automatically sense and react to their environments.
Ecosystem	A view in which components and their environment are part of a single system; often used to discuss organizations, devices and their environments	Providing value via IoT approaches requires that a large number of stakeholders come together (i.e., form an ecosystem). Parts of an ecosystem can be public, and other parts can be private.
Smart	Objects that can be physical or virtual and that interacts not only with people but also with other smart objects	Many IoT networks aim to achieve this principle.
Intelligent	Objects that are able to act independently	This is the goal of some IoT approaches.
Blockchain	Decentralized, shared and immutable storage technology that relies on peer-to-peer networks	Blockchains may provide interesting future applications in terms of decentralized, immutable storage.

Table2: Related concepts

5. Empirical study of Swedish agencies

5.1 Methodology

The empirical part of our research may be characterized as an explorative, qualitative study. Our research approach was motivated by the purpose and scope of the study, which is to compile topics of interest to different government agencies that in turn can be aggregated into themes or areas for focused research efforts. A qualitative approach is motivated by the multiplicity and complexities of agency responsibilities, together with the variations in relative significance of technology in different contexts. Moreover, a qualitative approach permits the elicitation of informed answers, enabling "in-depth studies […] in plain and everyday terms" (Yin, 2009, p. 6).

In keeping with the explorative nature of our study, our primary source of data was interviews with key respondents using "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 (e.g. reports). The focus of this empirical research was to build on the theoretical work presented in chapters 2 and 4 in order to discern the current readiness for – and perceptions of – IoT within Swedish agencies.

We analyzed first at the level of Swedish society and then drilled down into the activities of certain individual sectors: energy, food, transportation, health care, financial services, information and communication, and security. The semi-structured interview protocol and the generic invitation texts that were sent to prospective research participants are attached as appendices (Appendix2 and Appendix3, respectively).

5.2 Implementation

We approached the participating agencies (see table 3 below) either by directly contacting employees we believed to be knowledgeable about IoT and/or similar topics (e.g. digitalization), or by approaching the respective agency, outlining our interests and requesting that our inquiry be routed to a suitable department. While we found both approaches viable, the latter proved more time-consuming as general inquiries are ostensibly not given high priority. On more than one occasion, we had to send multiple inquiries (typically phrased as "kind reminders") before receiving a response.

Altogether, we conducted 16 interviews with individuals from 13 different agencies that represent seven different sectors: energy, food, transportation, health care, financial services, information & communication, and security. The number of respondents participating in each interview varied between one (13 interviews) and two (3 interviews). Interviews were conducted in two batches: one during late fall of 2017 and the second in the beginning of 2018.

Interviews were conducted via Skype or telephone as permitted by agency policy or respondent preferences. The interviews varied in length between 30 and 60 minutes depending on the role and insight of the respondent. 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 disparate structures, responsibilities and goals of the participating agencies, the notion of a strict interview manuscript was rejected. Instead, a semi-structured interview protocol was formulated drawing on theoretical work carried out at the start of the project, outlining six key areas of inquiry:

- IoT as a term
- IoT as an area of expertise
- Functionality and possibilities
- Current and future applications
- Challenges and risks
- Resources and security measures

Heeding these six themes permitted us to employ a common basis for all interviews yet while affording the flexibility needed to adapt to different topics, themes and examples brought up by the respondents.

The interview protocol was composed in English and in most cases (14 interviews) translated into Swedish in situ, as many of the respondents felt much more comfortable speaking in their native language. The remaining interviews were performed by the first author of this report and thus conducted in English in keeping with his language proficiency.

The analysis of the data material followed an interpretative approach (Walsham, 2006) whereby empirical data provided by respondents are interpreted based on the researcher's theoretical understanding of the research topic at hand. As such, the six areas of inquiry outlined above served to guide the analytical process by a) identifying relevant statements made by respondents and b) aggregating data from different sources into the results presented in chapter 6 of this report. The analytical process was supported by the use of Atlas.Ti – a software tool frequently in qualitative research to code data. Furthermore, Microsoft Excel was used for some additional tasks related to presentation and overview of data and results.

5.3 Participating agencies

To get an overview of the current situation at the sectors we conducted key respondent interviews across the different sectors. Table 3 lists the participating agencies divided into different sectors. We have anonymized the respondents to maintain confidentiality of the interviews. Respondents included unit leads, chief architects and managers with technical expertise.

Sector	#	Agency	Date
Energy	1	Energimyndigheten	Conducted Jan 9th, 2018
	2	Energimyndigheten	Conducted Jan 25th, 2018
Food	3	Livsmedelsverket	Conducted Jan 19th, 2018
Transportation	4	Trafikverket	Conducted Dec 5th, 2017
	5	Trafikverket	Conducted Nov 30th, 2017
Health care	6	Ehälsomyndigheten	Conducted Jan 23th, 2018
	7	Ehälsomyndigheten	Conducted February 2nd, 2018
	8	Sveriges Kommuner och Landsting	Conducted Jan 25th, 2018
Financial services	9	Skatteverket	Conducted Jan 12th, 2018
	10	Försäkringskassan	Conducted Dec 19th, 2017
Information and communication	11	Datainspektionen	Conducted Jan 16th, 2018
	12	Post- och Telestyrelsen	Conducted Dec 13th, 2017
Security	13	Totalförsvarets forskningsinstitut (FOI)	Conducted Jan 12th, 2018
	14	Lantmäteriet	Conducted January 30th, 2018
	15	Försvarets materielverk	Conducted January 30th, 2018 *Not recorded*
	16	Polisen	Conducted Dec 14th, 2017

Table3: Study participants

6. Cross-sector results

In this chapter, we outline the results of our study based on our six areas of inquiry. For results organized by sector, please see chapter 7.

6.1 Internet of Things as a term

During the course of our study, we asked the respondents to define the term Internet of Things. Furthermore, we asked whether their respective agency had adopted any official view on what that entails.

The results are conclusive with regards to the latter: No agency featured in our study has developed or adopted a shared, collective view on what the Internet of Things entails or how it should be defined. When asked about their individual perspectives, respondent views varied greatly as most of them were based on their respective area of responsibility. For instance, respondents from the transportation-sector offered fairly specific views that referred to devices installed in (or near) roads and railway tracks and facilitates proper operation of nation-wide infrastructure. Respondents from the food sector supervise inspection of facilities where food is either prepared, stored or transported. I their view, the idea of IoT is tightly coupled with the idea of moving away from manual, intermittent inspection to automated, continuous oversight. Respondents from the healthcare sector have a more service-oriented view, where the tools of the trade are increasingly digitized and able to increase both efficiency and reliability of health care.

The most encompassing and non-specific answers came from the security sector where the general consensus seems to be *just about anything that can be connected to the Internet*. This may also be regarded as in keeping with their responsibilities in that while furnishing a device or product with an Internet-connection provides opportunities for additional functionality, it also provides a means by misappropriate the device or access the system to which it is connected.

6.2 Internet of Things as an area of expertise

We asked the respondents participating in our study whether IoT is (explicitly or implicitly) regarded as a distinct area of competence. Furthermore, we asked whether the knowledge resources related to IoT are concentrated to one department or distributed across the organization.

Again, we can offer one conclusive answer in that no agency considers IoT as a distinct area of knowledge or expertise. The most compatible perspective may be found in the security sector where IoT and connected devices is not seen as an innovation as much as a variant on the existing issue of analyzing systems based on their ability to prevent unauthorized access. This perspective is perhaps most explicit in the agencies that are tasked to consider security from a

distinctly proactive perspective, i.e. what are the potential consequences of unauthorized access to the device itself? What harm can the hijacked device inflict upon its surrounding environment? It may be argued that the issue of connected devices has expanded the notion of environment to include not just the digital realm (i.e. other computerized systems), but also the physical realm in that a connected product (i.e. a vehicle) can cause physical damage.

As for the knowledge resources that underlie IoT, they are typically distributed across the organization – or not present at all. Respondents from at least one agency explicitly states that the overall IT capability in the organization is lacking and that it would take a significant investment in both technology and manpower to accommodate major technical innovations. One other agency states that they do have relevant knowledge resources in-house, but that their skill-set related to IoT is mostly incidental and related to individual interest or past working experience.

While it is difficult to provide categorical answers, the overall trend is that IoT-related skill sets are most prevalent *and* cohesive in the transportation- and information & communication sectors – albeit from different perspectives. The former supervises infrastructure that covers thousands of kilometers of road and rail and thus see tangible benefits from incorporating new technology and new devices to their benefit. Agencies in the information & communication sector do not apply technology in the same tangible sense, but are tasked with regulating their application. As IoT and connected devices attract more interest, these agencies see an increasing number of incoming questions regarding how existing rules and regulations can/should be applied in relation to new technology.

6.3 Functionality and possibilities

As part of our interviews, we asked the respondents what possibilities and advantages they perceived in relation to IoT.

While the responses were unanimously positive, they were in some cases immediately countered by possible risks (see more under 6.5). Furthermore, the perceived advantages were often vague; alluding to the ability of connected devices to provide more data that would in turn enables better service for citizens.

Respondents that see operational, short-term possibilities were able to provide more tangible use cases. In our study, we found that the food, transportation and health care offered clear ideas on how to improve their own sectors. The agency that represents the food sector in our study is among other things tasked with inspecting facilities where food is prepared, stored or transported. This task is very time-consuming in that these facilities are in many cases placed in remote locations, forcing inspectors to potentially waste several hours per day just travelling to and from the inspection site. A greater amount of automation (via connected devices) of routine inspections would free up a considerable amount of labor, which could be devoted to other (non-routine)

tasks. Furthermore, automated inspections could also alleviate the issue of reporting the results from inspections that currently take place on an annual basis. That is, the agency receives reports on inspections carried out by municipalities and counties at the end of the year in the form of huge data-files that takes months to compile and analyze. Hence, there can be anywhere up to a 15-month lag before the agency knows the results of an inspection – or indeed if it has been conducted at all. Greater automation of the inspection process could serve to severely shorten the delay from potential issue to agency awareness and response.

The example derived from the food sector hints at the possibility that IoT could enhance both efficiency in work processes and the quality of the results. Similar sentiments are echoed by health care and transportation where resources are also stretched thin. The health care sector sees connected, smart devices as an integral part to not only improving traditional healthcare, but also permitting citizens to caring for themselves with greater detail and reliability. This is especially relevant for citizens suffering from chronic conditions that require constant monitoring. The ability to supervise one's own condition is beneficial to the patient – who is able to retain much of their independence – as well as the caregiver that can divert its resources to where they are actually needed as opposed to performing routine tasks.

Respondents from the transportation sector discuss the same issues – efficiency and quality – in terms of reactive and predictive maintenance. The former is essentially what is often practiced today: when something breaks down – you effect repairs or replace it. This is typically more time-consuming as well as more costly as you have to dispatch technicians, wait for them to arrive, wait for damage assessments et cetera before repairs can even be initiated. Connected devices could conceivable provide invaluable information on the status of the infrastructure, permitting the responsible agencies to effect predictive maintenance, i.e. addressing a problem before it occurs. Respondents in the transportation sectors mentioned two distinct opportunities for this to occur. First, automated sensors can be installed and provide continuous information regarding the condition of road and rail. A second, and more interesting opportunity, is to access data from vehicles that are already utilizing the infrastructure. For instance, both trains and trucks are highly complex pieces of mechanical engineering that contain numerous sensors that gauge the condition of the tracks or road. Sharing some of this data with the respective agency would essentially mean that the vehicle is constantly reporting on the condition of the infrastructure that is being utilized.

6.4 Current and future applications

We asked the respondents if they could offer us any examples of how they apply IoT in their organization today. Alternatively, if they were in the process of implementing connected devices or similar technologies in the near future.

The overall impression is that IoT has not penetrated all that deeply into Swedish agencies. Respondents form the transportation- and security sectors

offered the most concrete examples of implementations that are currently in place. Respondents from the transportation sector are employed within an agency tasked with monitoring and maintaining long stretches of road and railway. As such, maintain some 700 automated weather stations that measure wind, temperature, humidity as well as ground frost in order to provide accurate and up to date information regarding local conditions throughout their infrastructure network. In addition, railroad exchanges have been fitted with sensors that monitor their position and operational status. If it takes longer than usual to switch between two tracks, then the exchange may require service or replacement.

The security sector also yielded a couple of examples of implemented IoT-related solutions. For the past couple of years, law enforcement utilize ANPR (Automatic Number Plate Recognition) in order to automatically scan the number plates of passing vehicles. Cars that are associated with legal infractions (e.g. reported as stolen) are flagged and alert law enforcement officers that this particular vehicle warrants attention. The authorities have also started installing specialized microphones in certain areas that register sounds that are essentially associated with criminal activity, e.g. broken glass or gunshots. The microphones do not register "normal" sounds such as conversations, but immediately alert law enforcement if there is reason to believe a crime is in progress.

Looking beyond these two sectors, there are sectors that see clear potential with connected devices and are gradually encouraging a movement towards IoT in whatever way they can. One example is the energy sector, which – not unlike transportation – is tasked with overseeing infrastructure that is essential to Swedish society. However, progress is slow as much of the infrastructure is owned by small, local actors that have neither the know-how nor the financial muscle to make large technical leaps. As a result, there is a clear difference in the level of technical development seen in larger, more affluent actors in the energy sector and smaller regional actors.

6.5 Challenges and risks

In our study, we asked the respondents about technical risks and general challenges associated with IoT. In an effort to cover as much ground as possible, we tried to solicit perspectives concerning the individual agencies as well as Swedish society as a whole.

In terms of general challenges, the situation facing the energy sector (see chapter 6.4 above) is essentially emblematic for most societal sectors. That is, embracing the IoT could *potentially* bring many advantages, but will *certainly* require significant investments in terms of time, funding and expertise. Government agencies are given certain areas of responsibility and certain goals that they should strive to achieve. While investments in IoT may well facilitate the accomplishment of said goals in the long run, they can prove difficult to justify in a short-term perspective unless there is a clear political mandate or motive to move in that direction. Furthermore, several respondents cited legal

restrictions as limiting the proliferation of IoT and similar “innovative” technologies. It is perceived that the legal framework is either unclear or obsolete and does not provide clear guidance regarding what is permitted in relation to utilizing “smart” technologies and digitizing tasks in order to enhance efficiency. The General Data Protection Regulation (GDPR), which is set to take effect in May 2018, is adding to the confusion and – at least temporarily – appears to be hindering the adoption of IoT while society as a whole evaluates its implications.

Turning our attention to the technical side of things, the two most cited concerns in our study are security risks and a lack of standardization. The former is ostensibly the most immediate deal-breaker for many agencies, with national defense being the most obvious example. The respondents we approached categorically stated that while connected equipment such as vehicles could feasibly provide may advantages (e.g. predictive maintenance), the risks associated with remote connectivity is simply unacceptable in military applications. In that context, any remote interface is essentially another possible means by which to render a vehicle or weapon useless, i.e. by replacing the corrupting the software that governs on-board systems, thus rendering the equipment useless.

The issue of standardization is also related to security in that there are many different suppliers of systems and devices that offer some form of remote connectivity, e.g. for the purpose of supervision or software updates. However, there are virtually no commonality in the interfaces used to communicate with different equipment. Each manufacturer seemingly develops and uses their own communication protocols. Moreover, these protocols typically offer very poor protection against unauthorized access. For instance, user information and/or passwords may be sent without any encryption whatsoever, making it very easy to intercept by third parties who could then use it to misappropriate the equipment in question – or even use it to access central systems at an agency. The need for secure – and mature – interfaces are especially germane for connected devices as they are more autonomous than digital devices such as desktop computers and smartphones. That is, they operate with little or no direct involvement by people, meaning that a breach of security may go unnoticed for comparatively long periods of time. The lack of standardization and safe protocols are cited by respondents in the transportation sector as a continuous source of concern as well as a driver of costs. While there are clear benefits to using connected devices to support Swedish infrastructure (see chapters 6.3 and 6.4), the lack of standardization and mature communication protocols means that agencies have to bear the cost of integrating (or even upgrading) individual connected devices into a cohesive system, severely hampering the applicability of IoT to support agencies in their mission.

6.6 Resources and security measures

Finally, we asked the respondents what resources that their respective agencies provide as well as what external resources they utilize in relation to IoT.

Furthermore, we inquired as to how they work to enhance security in relation to connected devices.

As our study revealed relatively few tangible resources aimed at supporting IoT in Swedish government agencies. The transportation sector exhibits the most extensive examples with the adoption of relatively mature integration platforms that can facilitate the integration of disparate connected devices into a cohesive, manageable system. Furthermore, respondents in this sector cited a relatively large IT-staff (encompassing over 1000 people) needed to handle integration and maintenance of connected devices. Maintaining in-house capabilities is also beneficial when formulating requirements in public procurement. Again, respondents in the transportation sector utilize carefully formulated, long-term contracts as incentives to push suppliers towards using standard protocols.

In addition to maintaining in-house IT-capabilities, several agencies cite participation in international networks or interaction with other agencies as a valuable source of knowledge input. For instance, respondents from the security sector name the European Cybercrime Centre (EC3)[11] – a part of Europol – as an important partner in relation to IT-based threats.

Looking beyond security-oriented resources, several respondents cited examples or use cases from citizens, other agencies or countries are valuable sources of ideas and inspiration. A respondent from the food sector illustrated this point by describing how our neighboring country of Denmark has invested heavily in technology that streamlines their inspections of facilities that produce and process pork, enabling authorities to quickly respond to any deviation from acceptable standards.

Finally, while the financial sector are not concerned with connected devices “in the field” in quite the same way as many of the other sectors, they are looking to what digitalization entails in the long run. Namely, a cash-less society with an increasing diversity of devices and electronic currencies (e.g. bitcoin) rather than cash as forms of currency and conveyors of financial transactions. With that in mind, they are actively working to develop new technical interfaces that make financial transactions facilitated via modern technology simple to use as well as compliant with Swedish laws and tax codes.

[11] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

7. Discussion

This chapter relates the findings of our study to the respective sectors featured in our study. We also discuss the perceived gaps in our current understanding of IoT based on empirical findings as well as a review of extant research.

7.1 Issues raised in different sectors

Table 4 provides a summary of our empirical findings organized by societal sector and five key concerns specified as of particular interest to the Swedish Civil Contingencies Agency (MSB). Chapters 7.1.1 – 7.1.7 provides additional detail regarding each sector.

	Functionality	**Threats**	**Risks**	**Protection**	**Integrity**
Energy	Increased energy data, tracking of energy usage, novel services based on consumption	Increased vulnerability, old equipment	Possible malfunctions have dramatic consequences	Regulation, standards, investing enough resources	Loss of personal energy data
Food	Increased location-based data of food, animals, automated inspections	Over regulation	Food security compromised	Regulation, investing resources	Data on individual farmers
Transport	Real-time location information, connecting infrastructure, providing third-party services	Over-reliance on technology	Transport infrastructure critical, break downs dangerous and costly	Controlling large parts of the infrastructure	Information on individual locations
Health	Better monitoring, scheduling, better performing processes	Equipment malfunction, corrupting data and processes	Direct consequences to well-being, dissemination of private information	Standardization, risk aversion, legal/ethical oversight	Severe concerns related to data quality, privacy, information security

Financial	More data to base financial decisions on	Unsafe services, technology taken into use	Fraud, losing funds, interruption of business	Regulation, investing resources	Financial data private
Information and communication	Guaranteeing working IoT infrastructure	Networks, internet breaking down, underestimating IT complexity	May have dramatic impacts depending on usage area	Regulation, (international) standardization, development of knowledge	Compromised networks do not guarantee privacy or data security
Security	Sensing, Recording, novel enforcement mechanisms, real-time information, dataficiation	Unwarranted surveillance, data stolen	Large-scale societal disruptions, societies breaking down.	Development of legal frameworks, regulation	Privacy and other fundamental rights violations

Table4: Summary of key issues per sector

7.1.1 Energy

Our study suggests that the energy sector demonstrates clear potential for improvement using IoT as a means to improve efficiency as well as maintain the energy infrastructure on a national level. Much of the energy infrastructure is comprised of relatively small actors that consider IT to a source of cost rather than an enabler of efficiency or improvement. These actors typically operate on small budgets and are often burdened with a significant debt in terms utilizing technology that was never intended to be remotely connected, or technology that is remotely connected, but not able to provide adequate security.

On the other hand, larger enterprise that operate on a national or international basis are able to leverage connected devices and other technologies that permit remote management and maintenance. In 2017, the International Energy Agency published an extensive report that outlines how the energy sector, including oil, coal and electricity, can leverage the forces of digitalization to enhance efficiency, provide a more secure infrastructure and create more flexible energy markets (IEA, 2017). A tangible example is the use of smart demand response-solutions that permit consumers to dynamically direct their energy consumption to coincide with off-peak hours – reducing their energy costs and lowering the overall burden placed on the distribution infrastructure.

Overall, the energy sector exhibits a wide disparity in its constituent actors. On one end of the spectrum, we have international energy companies that spend large amounts on research and development as well as investments in new technology. On the other end, we have small, municipal providers of district heating that operate on a tight budget and are ill-equipped to manage the large-scale investments needed to bolster efficiency and security.

7.1.2 Food

The food sector appears to be of two minds. One the one hand, government oversight is largely (if not entirely) based on manual inspections that are either conducted by different government agencies themselves, or by external actor that report to the respective agencies. The predominance of manual procedures are partially based on the pervasive culture and norms that govern "how things are done", but are also explicated in EU-regulations that specify that a certified inspector has to be on-site when inspections are conducted. Furthermore, inspection protocols are compiled on an annual basis, leaving the agency tasked with oversight with massive amounts of reports that take months to process and review. Hence, the sector as a whole is currently not able to quickly detect or respond to deviations from acceptable standards or practices.

On the other hand, the food industry is – much like every other aspect of our society – subject to digitalization and undergoing rapid change as retail of foodstuffs is often conducted online and delivered via carrier directly to the customer. Moreover, locally produced foodstuffs are increasingly being marketed and sold directly to customers online without passing through the industry's traditional value chain[12]. Agencies tasked with overseeing the food sector face a significant challenge in adapting to these novel business models and an increased presence of "smart" devices that can monitor and continuously report how food is stored and transported could be part of the solution.

7.1.3 Transportation

According to our study, the transportation sector appears to the most active in engaging with technologies and practices that fall under the general paradigm of IoT. This is largely due to an established tradition of working with – and relying upon – various forms of technology to either automate routine tasks or support procedures that require human discretion. Hence, there is an established view that connected devices can provide greater efficiency and enable new and better tools with which to oversee vast stretches of road and rail.

There are significant challenges associated with integrating systems, products and components delivered by different suppliers as there are few common technical standards or interfaces. Furthermore, protocols used for communication often exhibit poor security and could serve as a point of entry for unauthorized access to individual devices or even larger systems. Thus far, government agencies manage this issue by maintaining a comparatively large in-house IT-staff that can effect post-delivery improvements to connected devices before they are put into use. However, a more long-term strategy is to work closer with supplier and convince them to adopt (or help develop) secure,

[12] http://www.ehandel.se/Narproducerat-online-vaxer-premiar-for-Gardsbudet,7207.html

standardized interfaces. One means to go about this is to offer long-term contracts as incentives, providing a profit motive for suppliers to improve their products.

There is however a significant disparity in the level of standardization present in railroad and road networks. Railroad has historically been more tightly regulated and influenced by fewer actors. As such, the underlying infrastructure is relatively homogeneous. In comparison, roadside technologies are much more diverse as technical evolution has progressed on a city-by-city and project-by-project basis. Hence, it is presently much more feasible to oversee and develop supporting technologies for Swedish railway than roads.

One interesting possibility is the idea of essentially crowdsourcing supervision to the many vehicles that utilize road and rail infrastructure on a daily basis. Each train, commercial truck and to an increasing extent automobile carry a significant amount of on-board sensors and sophisticated systems that asses the vehicles surroundings. Hence, they are able to assess, e.g. based on speed, vibrations, temperature, rotational speed of wheels et cetera, localized conditions pertaining to weather, traffic congestion, road conditions or wear-and-tear on rail. Access to data generated by each vehicle travelling by road or rail in Sweden could provide government agencies with a wealth of information that could serve to support day-to-day operations as well as long term statistical analysis. However, realizing this idea on a large scale is no small undertaking and would require extensive reviews of current legal frameworks and development of palatable incentives to share data.

7.1.4 Health care

Health care in general, and care for outpatients and elderly citizens in particular, stand to gain significantly by increased use of new tools and technologies. IoT-oriented technologies are no different in that connected, “smart” devices can provide easy, round the clock access to healthcare personnel, e.g. via a simple alert button. Moreover, digitized medical tools, e.g. for gauging blood sugar levels or blood pressure, can enable citizens to monitor their own condition in the comfort of their own home without extensive medical training. The results of the respective tests can then – manually or automatically – be logged and presented as an online “diary” where citizens and medical personnel can monitor how a condition develops over time.

While the technical possibilities are plentiful, the health care sector deals with highly personal information and every procedural change or technical novelty has to be carefully evaluated. First, one must consider the rights to privacy of each citizen and how their integrity may be affected in the process of digitizing their medical information. While IoT is often said to enable supervision of equipment, e.g. in an industrial setting, applying the same language and perspective in a health care setting will no doubt cause offense. Second, there is the issue of established ethics and norms that govern medical practice. Patients and health care professionals rather than administrators, security experts or

programmers ultimately determine the boundaries of applying technology to support health care.

7.1.5 Financial services

While the financial sector is not actively pursuing the development of IoT for the purpose of improving or developing their internal processes, they are keenly aware of the rapid digitalization of society. Digitized methods for payment provides a tangible example as we are increasingly using credit cards or smartphones equipped with NFC (Near-Field Communication) or RFID (Radio Frequency Identification) technology to make purchases. Furthermore, cryptocurrencies like Bitcoin that were once considered suspect are gaining increasing legitimacy and is as of December 2017 traded on two exchanges.[13]

The main challenge for the financial sector is, simply put, to remain relevant in the eyes of these novelties. Our study hints at an emerging gulf in "digital maturity" based on how we conduct ourselves in our private life versus how we behave in our professional life. As private citizens we are relatively quick to adopt novel financial services based on their convenience or even the mere "wow-factor" of using something new. We are however considerably slower on the uptake in our professional lives where traditional financial institutions and forms of payment still prevail.

Government agencies tasked with overseeing the financial sector essentially have to accommodate both ends of the spectrum – traditional structures and new, digitally fuelled innovations. Failure to do so could result in the emergence of marketplaces or even whole economies that operate without any oversight – either intentionally (i.e. for criminal activity) or through sheer ignorance by unaware citizens. One of the respondents in our study went as far as to caution against a "democracy-deficit" where government agencies are not perceived as relevant in a modern economic landscape.

One means 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 will at the very least make it easier to develop new services that comply with existing financial regulations.

7.1.6 Information and communication

Much like the financial sector (see chapter 7.1.5), the information and communication sector finds itself responding to IoT and digitalization rather than working to apply it in their own organizations.

Their main challenge may succinctly be expressed as responding to a deluge of incoming queries from the private- and public sectors regarding what is and is not permissible. As the IoT is poised to encompass millions (or even billions) of connected devices distributed across multiple societal sectors (see chapter 2),

[13] https://www.svt.se/nyheter/ekonomi/bitcoin-nu-pa-tva-borser

we may surmise that the issue of uncertainty is not going away any time soon. Our study suggests that while there is no shortage of enthusiasm or "hype" surrounding technical novelties, there *is* a shortage of perspective and maturity in our legal frameworks. Recent events involving the Swedish Transport Agency (sv. Transportstyrelsen) clearly demonstrate that government agencies are not fully aware of the reprocussions of decisions related to IT-management.[14] New technical paradigms, such as IoT and before that cloud computing, tends to cause confusion regarding how existing regulations should be applied – or if they are applicable at all. However, while there is a perception that our existing laws need revising in order to reflect technical advances, our respondents stressed that people generally do not want *more* laws – they want more guidance regarding how to apply *existing* laws.

7.1.7 Security

Although security was raised as a major concern across all sectors featured in our study, we also interviewed respondents where security is tightly coupled with their professional, e.g. law enforcement and national defense.

A respondent from law enforcement highlighted that criminal activity is subject to digitalization just as much as any other aspect of our society. Just as we can apply technology to support health care or infrastructure, criminals can utilize technology to commit theft, fraud or worse. Responding to this development encompasses two distinct steps. The first step concerns how we can build devices and products that are harder to misappropriate (i.e. "hack") by unauthorized personnel. As it stands, this is largely up to the developers of connected products and government agencies can exert influence by either explicit requirements (i.e. in public procurement) or by facilitating a dialogue between actors in the public- and private sectors. The second step is more socio-technical in nature and concerns how technology – even if legally acquired – can be applied as a tool for different forms of criminal activity. (For instance, a kitchen knife may be legally purchased and used to prepare a meal. It may also be legally purchased and used as a weapon.) There is essentially an increasing need to work proactively rather than reactively in developing and evaluating different scenarios where technology can be used to the detriment of society or its citizens in different situations.

Finally, as our society becomes more digitalized and apply a wider range of IT-based tools in our work, government agencies also develop routines standards and routines for how to process information within one's department or organization. However, when faced with major incidents, agencies often have to work together and coordinate their efforts under difficult circumstances. The large fire that raged in Västmanland in 2014 provides a concrete example.[15]

---

[14] https://www.svt.se/nyheter/inrikes/utredare-transportstyrelsen-saknade-kunskap

[15] Several agencies have published reports on the incident. See https://www.msb.se/sv/Om-MSB/Sa-arbetar-

Hence, while the need for *technical* standards were brought up in multiple sectors, there is also a need for standards that regulate *inter-agency activities* and safeguard information integrity and security – even under chaotic conditions.

7.2 Knowledge gaps in extant research

IoT research is scattered across different sciences. There is a need to further investigate approaches to the related technological and social landscape; to draw together the different research streams and conduct multidisciplinary research. Currently these efforts are complicated by different levels of analyses and different research traditions and methodologies used in the previous studies. Both applied and more theoretical research are needed.

In information systems and management, IoT-related research is scattered. However, more work that would directly deal with IoT-related questions is called for. Some potential examples of related areas in information systems include:

- eGovernment work has a long history of focusing on the different stakeholders involved in technological transformation of services in society.
- Work on digital infrastructures focuses on topics, such as how novel technologies become infrastructure, and could focus on IoT.
- Studies in innovation and innovation management deal with how research and development activities in organizations and society can be organized to support implementation of novel technologies, for example IoT.
- Different forms of institutionalism and institutional theory are concerned with institutionalization of technology, and such approaches would be very fitting for IoT approaches.
- Work on social aspects of security have been investigated in information systems, but more such research is called for when the technology and use cases develop.
- Design science and active design science experiments offer an interesting potential for the possibility to simultaneously test new technologies and standards while reflecting back to the discussions on business model changes and process changes in the relevant sectors.

Local contexts are largely missing from IoT research, even though national regulation activities of the public sector and legal environment vary between

MSB/Regeringsuppdrag/Skogsbranden-i-Vastmanland-2014/Utredningar-och-utvarderingar/

countries. More research is needed in this area, for example the institutional setting of the Nordics may prove beneficial.

Many public sector organizations are moving forward swiftly in their digitalization initiatives and strategies. Usually these initiatives contain element of IoT for a particular sector. However, often there is a clear disconnect between these initiatives and the current academic research on the topic. Increasing links between these public and private sector initiatives and academia in terms of research and teaching seems worthwhile. Digital transformations in the different sectors of society require a strong foundation, including linkage to research-based knowledge and expertise.

Technical advances related to the devices and connectivity happen so quickly that the research has trouble keeping pace with these developments. The bigger picture of institutions and governance does not change so fast. There is often a considerable, unclear area of what is legal and ethical versus what would be technologically possible, for example issues related to personal privacy, data security, integrity, etc.

8. Recommendations for future research

In recent years, novel technologies and research on IoT have leaped forward. At the same time, different national organizations have developed their strategies going forward. This state-of-the-art report provides an overview of the Swedish national agencies based on a literature review and empirical research divided into seven different sectors: energy, food, transportation, health, finance, information, and communication and security.

Based on in-depth interviews and investigation of strategic documents in the different sectors, we find that, currently, sectors have a range of different initiatives, which are mainly driven forward independent from one another.

Strategy work related to IoT at the agencies is seen as important, but currently only some agencies have definitions and developed ways of working strategically with IoT. Knowledge and expertise on the topic is often scattered across organizations. Different agencies have very different resources to allocate and levels of ambition related to IoT.

There was some disagreement of how to define and discuss IoT meaningfully, especially when discussing the organizational impacts of technology, i.e., we found significant differences of expectations of the exact role IoT will play in the different sectors. One example of disagreements was related to the roles private and public actors will play going forward.

8.1 Example research areas

We propose further sectorial research efforts to security and privacy challenges IoT provides to Swedish agencies. We believe that including both private and public actors will help find long-term solutions and mitigate the risks for Sweden. Different agencies will need to continue developing capabilities for their own sector as well as try out ambitious—and even daring—pilots.

IoT technologies can be effectively combined with other technological developments such as artificial intelligence, cloud-based services or blockchain storage. In such settings the combination of several technologies offers novel opportunities, but also exposes to new risks.

We also propose cross-sector initiatives drawing on recent research—especially in the areas of **continuous digitalization**, **multi-stakeholder ecosystem governance,** and **inherent technology risks**—will be needed to address the challenges raised in this report. We also propose future comparative studies in terms of national IoT strategies carried out with neighboring countries, for example Finland, Estonia, and Norway.

8.2 Example future research avenues

Below we list some of the possible issues raised during our work and some related example research questions for the future. We have elected to raise issues related to three different categories: continuous digitalization, multi-stakeholder ecosystem governance, and inherent technology risks.

Continuous digitalization was apparent in all of the sectors discussed. This transformation means that public actors are currently in the process of doing wide-scale investment in digital technologies that will have dramatic effects on how their work is conducted (roles, processes, etc.). Thus, current and future IoT initiatives take place against a backdrop of large-scale transformation regarding how services are offered in the future.

This means that IoT-developments are often seen as only a small part of other digitalization advances and that their role might be complementary to other technologies. Examples include, IoT sensors as a method for gathering more accurate data related to health so that timely, quality care can be provided, and sensors tracking location-based data in cloud ecosystem providing data into distributed databases (blockchain).

Example research questions in this area would be, for example: *How do we conduct design experiments that build on existing IoT approaches?* and *How is IoT taken into account in public organization strategies?* What are good examples and cases to draw in this space?

Issues related to ***multi-stakeholder ecosystem governance*** were raised and identified in the sectors of health, food, and security. Related issues were discussed with several other respondents. The primary issue is related to the complex ecosystems that are needed for wide-scale adoption of IoT devices and services offered on top of those devices. These kinds of settings have a multitude of different public and private actors that may have partly unaligned aims. Of note, the tension between providing interoperability to treat service providers equally may contrast with the immediately-pursued commercial benefits of the private vendor providers and consults. Many of the interesting developments in this area are related to questions of standardization, ways to align stakeholder interests, and building sustainable governance models for these kinds of ecosystems.

Example research questions would include for example: *What IoT infrastructure can be served as open platform?, What should remain in the hands of the platform owner?* or *What are the roles of public sector agencies for IoT projects? How to organize public-private IoT project?* In general, it is unclear *should*, and if yes*, how, IoT devices be regulated somehow in a centralized manner?* Questions related to processes of sharing of information between agencies related to security was also raised.

We see also the current issues of **inherent technology risks** to impeding proliferation of IoT in Swedish agencies. This is especially evident in security, transport, energy and financial sectors where respondents identify several challenges of these kind facing their organizations.

Several novel attack vectors make IoT devices more vulnerable and the connected nature of the technology, ecosystem and overall complexity increases the risks involved. Both accidental and intentional threats can be identified, but mechanisms are needed to mitigate these risks in the ecosystem better.

Possible topics to be researched further would be directly related to security, for example *to the physical security of the devices or network-level security measures that can be taken to reduce vulnerabilities*. It is also a bit unclear who should be the major actors regarding IoT security and *what organizational and socio-technical changes would help to reduce vulnerabilities*?

It is worth noting that other countries and their public sectors are also struggling with similar topics. International research literature and empirical research in cross-border settings might thus offer interesting insights. One especially interesting area for further research would be to combine local challenges related to IoT to the UN global development goals [16].

[16] https://www.globalgoals.org

9. Feedback from respondents

A complete draft of this report was distributed to the participating respondents (see chapter 5) in April 2018 with an invitation to provide feedback and/or comments. Three respondents replied to our message. The first two merely acknowledged the report and said they had nothing to add. The third responded provided a number of detailed comments pertaining to their own particular societal sector as well as the overall report. A few of the comments have been incorporated into the final version of this report, while others have been considered but ultimately not included. The most common reason for exclusion is simply a matter of scope where this study is intended to provide an overview and a *starting point* for further research rather than a comprehensive account of all societal sectors and their use of IoT. However, as it is not our wish or intent to censor feedback from participants, we will list the comments that we did not address in our report.

- Report should use the expression ICT rather than IT
- Why does the report limit international comparisons to Finland, Estonia and Norway? The European Union have conducted significant work on issues pertaining to security and digitalization.
- Report recommendations for future research should place greater emphasis on platforms and scalability.
- Reduction of vulnerabilities are not limited to “network-level security measures”, but also discovery, management and containment of incursions. It’s a matter of assessing risks and what merits investments.
- The notions of “international threats” and “attack vectors” are too unspecific. Discussing IoT security without first outlining types of threats is a clear limitation to your report. A deeper analysis of threats and responsibilities would be greatly beneficial.

We, the authors, acknowledge these comments and feel that the issues raised by the respondent all deserve further attention in future research.

10. References

10.1 Research references

Ashton, K. (2009). That 'internet of things' thing. *RFID journal*, *22*(7), 97-114.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787-2805.

Atzori, L., Iera, A., & Morabito, G. (2014). From 'smart objects' to 'social objects': The next evolutionary step of the internet of things. *IEEE Communications Magazine, 52*(1), 97-105.

Bandyopadhyay, S., Sengupta, M., Maiti, S., & Dutta, S. (2011). Role of middleware for internet of things: A study. *International Journal of Computer Science and Engineering Survey*, *2*(3), 94-105.

Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications, 54*, 1-31.

Christensen, C.M., Raynor, M.E., McDonald, R.: What Is Disruptive Innovation? Harvard Business Review Digital Articles, (2015)

Da Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on industrial informatics, 10*(4), 2233-2243.

de Reuver, Sørensen C, and Basole R C (2017). The digital platform: a research agenda. *Journal of Information Technology*. Article In Press.

Dong, L., Shu, W., Sun, D., Li, X., and Zhang L. (2017). Pre-Alarm System Based on Real-Time Monitoring and Numerical Simulation Using Internet of Things and Cloud Computing for Tailings Dam in Mines, *IEEE Access,* vol 5.

Dijkman, R. M., Sprenkels, B., Peeters, T., & Janssen, A. (2015). Business models for the Internet of Things. *International Journal of Information Management, 35*(6), 672-678.

Ghazawneh, A., and O. Henfridsson (2013). Balancing platform control and external contribution in third-party development: the boundary resources model. *Information Systems Journal, 23*(2), 173-192.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645-1660.

Lee, J., Bagheri, B., & Kao, H. A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing Letters*, *3*, 18-23.

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons, 58*(4), 431-440.

Lee, A. (2001). Editorial. MIS Quarterly 25 (1): iii-vii.

Lu, Y., Papagiannidis, S., & Alamanos, E. (2018). Internet of Things: A systematic review of the business literature from the user and organisational perspectives. *Technological Forecasting and Social Change*. Article In Press.

Lyytinen, K. and L. King (2006). Standard Making: A Critical Research Frontier for Information Systems Research. *MIS Quarterly, 30*, Special Issue on Standard Making, 405-411.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad hoc networks*, *10*(7), 1497-1516.

Ng, I. C., & Wakenshaw, S. Y. (2017). The Internet-of-Things: Review and research directions. *International Journal of Research in Marketing, 34*(1), 3-21.

Oliva, R., & Kallenberg, R. (2003). Managing the transition from products to services. *International Journal of Service Industry Management, 14*(2), 160-172.

Pang, R., Chen, Q., Han, W., and Zheng, L. (2015). "Value-centric design of the internet-of-things solution for food supply chain: Value creation sensor portfolio and information fusion", Inf. Syst. Front., 17, 2, (Apr 2015): 289-319.

Parker, G. and Van Alstyne, M. (2017). Innovation, Openness, and Platform Control. *Management Science, online in articles in advance*.

Saarikko, T., Westergren, U. H., & Blomquist, T. (2017). The Internet of Things: Are you ready for what's coming?. *Business Horizons, 60*(5), 667-676.

Scott, W.R.: Institutions and Organization: Ideas, Interests, and Identities. Sage, Thousand Oaks (2014)

Suo, H., Wan, J., Zou, C., & Liu, J. (2012, March). Security in the internet of things: a review. In *Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on* (Vol. 3, pp. 648-651). IEEE.

Stojkoska, B. L. R., & Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production*, *140*, 1454-1464.

Thomas, L., Autio, E., & Gann, D. (2015). Architectural leverage: putting platforms in context. *The Academy of Management Perspectives, 3015*(1), 47-67.

Tilson, D., K, Lyytinen and C. Sørensen (2010). Digital infrastructures: The Missing 15 Research Agenda. *Information Systems Research, 21*(4), 748–759.

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems*, *15*(3), 320-330.

Van Alstyne, M., Parker, G. and Choudary, S. (2016). *Harvard Busienss Review, 94(4), pp. 54-62*.

Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. *Information Systems Frontiers, 17*(2), 261-274.

Wuenderlich, N. V., Heinonen, K., Ostrom, A. L., Patricio, L., Sousa, R., Voss, C., & Lemmink, J. G. (2015). "Futurizing" smart service: implications for service researchers and managers. *Journal of Services Marketing*, *29*(6/7), 442-447.

Xu, L., He, W., Li, S. (2014). Internet of Things in Industries: A Survey. *Transactions of Industrial Informatics 10, 4, 2333-2243*.

Yin, R. K. (2009), *Case study research: Design and methods*. 4th edn. Sage Publications, Thousand Oaks.

Yoo, Y., Boland Jr, R. J., Lyytinen, K., & Majchrzak, A. (2012). Organizing for innovation in the digitized world. *Organization Science, 23*(5), 1398-1408.

Yoo, Y., Henfridsson, O., & Lyytinen, K. (2010). Research commentary – the new organizing logic of digital innovation: an agenda for information systems research. *Information Systems Research, 21*(4), 724–735.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things journal*, *1*(1), 22-32.

10.2 Other relevant reports

Gartner, Inc. (2015). Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015, Retrieved from: http://www.gartner.com/newsroom/id/3165317

International Energy Agency (2017). Digitalization & Energy. Retrieved from: http://www.iea.org/digital/

The Economist Intelligence Unit. (2013). The Internet of Things business index. In Technical report. London, UK: The Economist Intelligence Unit.

Manyika, J., Chui, M., Bughin, J., Dobbs, R., Bisson, P., & Marrs, A. (2013). Disruptive technologies: Advances that will transform life, business, and the global economy (Vol. 12). New York: McKinsey Global Institute.

Schlautmann, A., Schelb, K. & Berguiga, M. (2015). Connecting the dots: Telecommunication providers as enablers for smart cities. Brussels: Arthur D. Little

Appendix 1: Key technologies

Name of the technology	Short description of the technology
Actuator	Component responsible for movement and control of a device, i.e. a railroad exchange.
Bluetooth	Radio-based wireless standard to exchange data.
Cloud computing	To use network of remote servers to host data or applications (over the Internet).
GPS	Global Positioning System. Global navigation satellite system providing time and location.
IP	Internet Protocol. Packet-based transfer protocol and addressing system.
Ethernet	Computer networking technology developed for local area networks.
NFC	Near Field Communication. Close proximity wireless connection protocol that does not require internet connection.
P2P	Peer to Peer. Distributed connectivity architecture that helps to partition of workloads and tasks among peer (nodes).
Sensor	Device that detects events in the environment and communicates this information.
Smart meter	Device that records consumption of energy.
SOA	Service-Orientated Architecture. Way to provide specific software services over a network.
RFID	Radio-Frequency Identification. Identifies and tracks tags attached to objects via electromagnetic fields. Can be active or passive.

Table1: Non-exhaustive list of key technologies enabling IoT

Appendix 2: Example letter

Letter format 1

Kort om vem jag är och varför jag kontaktar Er: Mitt namn är XXX och jag är verksam som postdoktor vid Göteborgs universitet, institutionen för tillämpad IT. Jag deltar för närvarande i en studie finansierad av Myndigheten för Samhällsskydd och Beredskap som syftar till att kartlägga svenska myndigheters syn på Sakernas Internet (eng: Internet of Things, IoT).

Studien är tänkt att generera en aktuell bild av definitioner, synsätt på och säkerhetsutmaningar med Sakernas Internet med fokus på funktionalitet, hot, risker, skydd och integritet. Syftet med denna översikt är att bättre kunna rikta framtida forskningsinsatser mot områden som är relevanta för såväl samtida som framtida utmaningar för samhället. Mot bakgrund av detta undrar jag om Ni är intresseradeav att bidra med Ert perspektiv på Sakernas Internet och hur det påverkar –eller förväntas påverka –[er verksamhet].

Jag tänker mig en intervju som omfattar 30-45 minuter vilken vi kan genomföra fjärrledes via Skype/telefon alternativt att jag besöker ert kontor om det är praktiskt. All hjälp i detta ärende skulle uppskattas.

Med Vänlig Hälsning,

Appendix 3: Interview protocol

We are researchers at GU who are conducting a survey regarding the perception of the IoT (Sakernas Internet) within Swedish government agencies. This study is funded by Myndigheten för Samhällsskydd och Beredskap.

Part of the discussion will concern your views on the IoT.

We would like to record this conversation for research purposes; the recording will not be posted anywhere. We anticipate that the interview will last 30-45 minutes.

BACKGROUND

Sector, agency

Purview of the agency

Person – position and professional experience

Experience with the topic

What does the IoT mean…

- To you?

- To your agency?

This is our preliminary definition of the IoT: Internet-connected devices equipped with sensory capabilities that are capable of capturing real-world occurrences.

Examples:

- A connected washing machine that sends alerts when it breaks down.
- Motion sensors that regulate the need for ventilation in an office.
- Connected vehicles equipped with a multitude of sensors that enable various driver-support systems and that inform the manufacturer of the vehicle's performance.

What are the main challenges…

- For Sweden?

- For your sector?

What are the most important security implications?

- Threats (tampering)
- Risks (systemic failures or accidents)

What security mechanisms do you employ?

Is privacy an issue? How do you deal with it?

Who are the most relevant actors in the field?

(How do you find information on IoT? Do you use domestic sources? Do you use international sources?)

Does the authority provide resources or (legal) regulations for the IoT? If so, what resources or regulations does it provide?

- What are the roles of the public and private sectors?

What initiatives or projects are you conducting in the IoT area?

What are the functionalities of the IoT devices you use? Describe the hardware affordances and software settings.

What technologies do you apply in these projects? (If possible, provide separate lists for each project.)

Do you have any dedicated IoT staff members (experts) or departments?

(Is the IoT considered a dedicated area, or are capabilities diffused throughout the organization?)

What IoT knowledge gaps have you identified in your field or agency?

What benefits do you expect to derive from IoT?

(What direct costs and savings are involved with the IoT? What about public costs?)

How do you deal with the IoT in the public procurement process? (Give technical and functional specifications.)

Would you like to add anything? Is there anything relevant that we did not discuss?

Should we talk to anyone else in your organization or sector about the IoT?

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB1194 – April 2018 ISBN 978-91-7383-817-7