CSS CYBER DEFENSE PROJECT

Trend Analysis

The Challenges of Scaling the Internet of Things

Zürich, August 2019

Risk and Resilience Team
Center for Security Studies (CSS), ETH Zürich

Author: Alice Crelier

Contact:
Center for Security Studies
Haldeneggsteig 4
ETH Zurich
CH-8092 Zurich
Switzerland
Tel.: +41-44-632 40 25
css.info@sipo.gess.ethz.ch
www.css.ethz.ch

Analysis prepared by: Center for Security Studies (CSS), ETH Zurich

ETH-CSS project management: Tim Prior, Head of the Risk and Resilience Research Group, Myriam Dunn Cavelty, Deputy Head for Research and Teaching; Andreas Wenger, Director of the CSS

Please cite as: Alice Crelier (2019) Trend Analysis: The Challenges of Scaling the Internet of Things, August 2019, Center for Security Studies (CSS), ETH Zurich.

Table of Contents

Executive Summary

Objective and methods

Over the past ten years, experts, lawmakers, governments and organizations have become more and more interested in the Internet of Things (IoT)[1] and individual smart and connected devices (IoTs), addressing the topic in various scientific and journalistic papers as well as in policy statements and bills. This new dynamic can be traced back to two overarching developments: First, the rapid evolution of Information and Communication Technologies (ICT) allowed IoT-related production costs to drastically decrease. This consequently led to an IoT boom across the industry, ranging from connected cars and smart homes to smart toys and wearables. Essentially everything – from life-saving inventions like automated health systems to the most inutile "smart" toilet paper hanger – could be turned into a smart device. Second, the IoT boom opened the door to various IoT-related intrusions or breaches. Indeed, the large number of unsecured IoT devices, the immense network they are part of, and the cumulative computing power of millions of IoT devices formed a fertile breeding ground for powerful, disruptive and intrusive botnets like Mirai and various intrusions like, for example, penetrations into industrial robots or connected cars. Consequently, since 2009, the increase in threats and security incidents has pushed civil society and international organizations to find ways to regulate the field.

A review of relevant literature revealed five overarching trends. First, there is no clear definition of the IoT. Second, businesses selling IoT devices are flourishing. Third, IoT devices have increasingly become targets and vehicles of choice for perpetrating data breaches and Distributed Denial of Service[2] (DDoS) attacks, and compromising networks. Fourth, academic research within this field has shown that, as of today, an alarming number of IoT devices are unsecured or already obsolete and no longer supported. Fifth, calls to comprehensively regulate the IoT landscape are increasing.

In light of these five overarching trends, this paper aims to find answers to the following questions: What is the IoT really about? Why has it become this trendy? What are the most common vulnerabilities in IoT devices? Why do these vulnerabilities still exist? And why is the implementation of efficient IoT-related regulation taking so long?

Findings

Research on the contextualization and definition of the IoT and IoT devices has led to a holistic definition of the IoT as a cyber-physical array of trans-sectoral[3] pervasive network-ecosystems which is made up of the interconnection of multiple IoT devices and the data they share via ICT.

Moreover, this Trend Analysis (TA) defines the IoT as a trans-sectoral and societal phenomenon that is present in almost all aspects of daily life and affects all sectors of society. In this regard, this TA defines IoT devices as all physical and virtual connected devices which sense, compute and interact with each other without any human intervention.

This definition establishes a frame for reflecting on the challenges which the IoT poses to our society. Research results have highlighted that the reasons for the hype around IoT devices (cheap to produce, trendy and deployable in any societal layers) are also the reasons for the IoT being so vulnerable. Indeed, further research has led to the conclusion that the economic dynamics of the IoT are responsible for the security and safety problems the IoT is facing

Prominent IoT-related incidents have highlighted how poorly secured IoTs are, even when it comes to automated industrial systems, critical infrastructures and even the defense sector. This chapter raises the issue of the need for IoT regulation.

However, word occurrence analyses executed on publicly available English-language government cybersecurity and cyberdefense documents highlight that the vast majority of countries, including the United States of America (USA) and China, do not conceptualize the IoT in their strategies. IoT-related implications for the defense sector are again addressed in this context. Finally, it seems that governments, civil society and international organizations are unlikely to implement coercive or compulsive regulations regarding the IoT.

Disclaimer

Data for this Trend Analysis was drawn from available open-source material. National cybersecurity and defense strategies that were not publicly accessible were excluded from the dataset.

Moreover, many IoT-related incidents or demonstrations, both in the private and public sector, go unreported due to fear of reputational damage. As a result, building a complete dataset of international incidents is impossible. The incidents catalogued here are already in the public domain and are well documented in cybersecurity and defense media reports. As a result, the dataset used in this TA is representative and sufficiently comprehensive to draw the conclusions presented in this document.

[1] Abbreviations are listed in section 9 at the end of the document.

[2] Technical terms are explained in a glossary in section 8 at the end of the document.

[3] In this TA, trans-sectoral stands for a phenomenon that reaches all sectors of society.

1 Introduction

The Internet of Things (IoT) [4] is not a new paradigm, however, it gained importance with the evolution of Information and Communication Technologies (ICT), decreasing production costs and the broad automation of the industrial sector. The IoT has reached all societal layers and sectors, from security to health. Businesses surfing on the trend of so-called “smart objects” are increasingly targeting consumers’ daily lives. This trend has led to the production of both widely adopted connected devices (IoTs) such as sports wearables and unique IoTs such as connected trash cans. However, concerns over the security of IoT devices were confirmed in 2016 when the Mirai malware infected an unprecedented number of vulnerable IoT devices to create one of the largest botnets ever known. Between August 2016 and February 2017, Mirai was used in several Distributed Denial of Service [5] (DDoS) attacks around the world. These attacks will be addressed in section 5.1 (Associated Press, 2017; Franceschi-Bicchierai, 2017a; Szoldra, 2016; Untersinger, 2017). Due to both its scale and disruptive potential, Mirai became a trigger causing governments, international organizations and civil society to finally consider IoT-related security vulnerabilities.

Although the literature is extensive and covers many aspects of the IoT, a generally accepted definition is still lacking. According to the literature, the rather vague and all-embracing concept of the IoT is difficult to regulate at the national and international level from a technical and legislative point of view, thus paving the way to loose security standards and practices (Arashi et al., 2017; ENISA, 2017; Kleinhans, 2019; Openshaw et al., 2014; Paratus People Limited, 2018; Sattler, 2019; Tonin, 2017a). This ultimately gives rise to the following concerns:

The available literature addresses security and privacy aspects of IoT devices that manufacturers commonly neglect. Indeed, articles highlight the fact that the number of IoT devices is growing exponentially and that the deployment of such technically unsecured devices in homes, industries and critical infrastructures constitutes both a serious security risk and an acute societal challenge (Bode, 2018; Bur, 2017; Dabbagh and Rayes, 2017; Kleinhans, 2018; Lewis, 2016; Tonin, 2017).

Moreover, a central characteristic of IoT devices is that they use sensors to gather, process and analyze private data, and there are also security concerns regarding the use and share of this collected data (Fu et al., 2017). The literature further examines the possible use of IoT devices in the military and defense sectors. Reports describe domains in which IoTs are already employed and suggest new domains in which they could be developed and used to improve military operations (Fraga-Lamas et al., 2016; Tortonesi et al., 2016; Zheng et al., 2015).

All of the above-mentioned trends indicate that the IoT poses several challenges to society, which will be addressed as follows in this TA:

Section 2 of this paper aims to establish conceptual homogeneity regarding the IoT and its connected devices. To do so, this report contextualizes and defines the IoT and highlights its multi-layered and trans-societal nature. By doing so, this TA develops a conceptual framework that furthers our understanding of what precisely makes the IoT both a market hype and a societal challenge in terms of its security and safety.

Section 3 highlights the reasons why the IoT is in vogue and how it benefits society.

Section 4 analyzes the most noteworthy economic trends of the IoT to elicit the reasons that lead manufacturers to produce poorly secured and unsafe IoT devices. To do so, this section first explains the market’s trade-off between costs and security in regard to the IoT. The section then addresses the lack of awareness and the concept of information asymmetry related to the IoT. The third part of this section outlines the dysfunctional standard design of IoT devices as well as their production processes and lifecycle management.

Section 5 summarizes IoT-related vulnerabilities and prominent incidents to bring to light the extent of risk inherent in the misuse of the IoT.

Section 6 explores the current state of national and international regulation regarding the IoT.

Section 7 addresses the aforementioned topics with regard to the defense sector and armed forces.

Finally, section 8 is dedicated to conclusions and further considerations regarding IoT-related societal challenges.

This Trend Analysis is based on an extensive literature review and analysis of a wide spectrum of policy papers, journalistic coverage and academic literature.

[4] Abbreviations are listed in section 9 at the end of the document.

[5] Technical terms are explained in a glossary in section 8 at the end of the document.

2 Contextualizing and Defining the IoT

Discussions of IoT security policies are taking place in many different contexts, ranging from industry, IT security companies, international organizations, (such as the International Organization for Standardization (ISO), NATO and the EU) to national bills and strategies. However, given the increasing number of organizations expanding into the IoT policy space, a single unifying definition of the IoT is naturally lacking. The debate surrounding the possible inclusion of smartphones and tablets as IoTs best illustrates this definition gap: While some authors consider smartphones and tablets – which contain up to 10 embedded sensors – to be "*the ultimate IoT devices*", others believe that smartphones and tablets do not constitute IoT devices (Duffy, 2014; Hausenbla, 2014; Khaddar and Boulmalf, 2017).

In order to strip away the ambiguity linked to the concept of the IoT, this section aims to contextualize and define the IoT and IoT-connected devices from a holistic perspective, which is better suited to a broader systemic and socio-economic approach. Indeed, a holistic approach emphasizes the importance of the whole system and the interdependencies within it rather than breaking it down into parts. When referring to the IoT, a holistic approach is able to highlight the systemic complexity of the phenomenon and produce a broader perspective regarding its technical and societal definition.

Consequently, this section will look into the literature and its main debates regarding IoT definitions and conceptualizations. It first contextualizes the evolution of the IoT concept before highlighting the fundamental characteristics of the IoT and IoT-connected devices to finally define them for this TA.

2.1 Origins and Evolution of the IoT Concept

The first use of the IoT concept goes back to 1999, when Kevin Ashton, Executive Director of the Auto-ID Centre at the Massachusetts Institute of Technology, explained the various possible applications of radio frequency identification (RFID) in supply chain management (Ashton, 2019; Jia et al., 2012; Tonin, 2017b). Years later, the broad democratization of the Internet and the evolution of means of production in keeping with the information society made the notion of the IoT considerably more feasible. Indeed, given the existing, widely increased interconnectivity, technological advances (e.g. the implementation of IPv6, miniaturization, etc.), and machine-to-machine (M2M) communication, the concept of the IoT has started to encompass the multi-layered, multidimensional, multi-sectoral and decentralized attributes of our complex contemporary reality (Rifkin, 2012; Ruche, 2019; Toffler et al., 2011).

As early as in 2005, the International Telecommunication Union (ITU) proposed a definition of the IoT as *"the ubiquitous network technology integrating goods with the Internet, such as sensor and radio frequency identification devices (RFID) technology*" (ITU, 2005). In 2012, the ITU issued a slightly different version of its definition of the IoT as "*a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies*" (ITU-T, 2012, p. 1). In 2017, the European Union Agency for Network and Information Security (ENISA) defined the IoT as "*a cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making*"(ENISA, 2017, p. 18).

These definitions of the IoT have been chosen because they reflect the overall status of the literature in the field at the time of their publication. Moreover, they emanate from international institutions like NATO or the ITU are likely to influence future national strategies due to their institutional legitimacy.

When contextualized, these definitions highlight the following trends: First, the societal context in which a definition is produced determines how inclusive or holistic the resulting definition is. Consequently, technical definitions of the IoT tend to be more exclusive while non-technical definitions are often inclusive.

While too little inclusiveness can lead to technical definitions that fail to address societal implications, too much inclusiveness can lead to vague or ambiguous definitions. The challenge here is to conceptualize the IoT and its definition with a sound balance between technical and societal aspects.

Second, this Trend Analysis noted a continuous shift towards a less technical and more inclusive definition of the IoT. Back in 2015, when Ashton conceptualized the IoT, he did so in a technical context. His definition was consequently technical and aimed at a predominantly technical audience. Compared with Ashton's definition, the ITU's above definition of the IoT would be a good example of so-called "umbrella terminology". However, definitions like ENISA's and ITU's illustrate the ongoing shift from exclusiveness to inclusiveness; from mainly technical to political, sociological and economic approaches. They emanate from political, sociological or economic contexts and are aimed at a political, sociological or economic audience.

Rapid technological development of the IoT and IoT-related broad marketing have raised questions about IoT vulnerabilities and regulation at the political as well as strategic level. As a result, the IoT, like cyberspace, has become a multifaceted societal phenomenon embracing all societal aspects, from health to defense.

2.2 Defining the IoT

As explained above, the IoT can be found almost everywhere. The market[6], surfing on this trend competes for the buzz of coming up with new benchmarks like "*the Internet of Everything*", "Cyber-*Physical Systems*", or "*Smart-things*" (Tonin, 2017). However, at its core the concept of the IoT is about interconnectivity, data collection, optimization and society.

In other words, the IoT is about communication, network infrastructure, connected devices and big data collection. The fundamental characteristics of the IoT can be described as follows:

Communication protocols, in regard to the IoT, must guarantee the reliable and structured transmission and reception of information and ensure interoperability of networks, no matter the location of the services (ENISA, 2017; Ochs, 2017). This interconnectivity is essential for the IoT, and the context of use defines the communication protocols and the combinations in which they will be used.

The network is the physical infrastructure enabling the layered communication between IoTs and/or the IoT ecosystems nodes within the IoT. This infrastructure can be wired or wireless and can be based on the Internet Protocol (IP) or not (e.g. Ethernet, USB, ZigBee, Bluetooth, 5G, GPS, SMS, Radar, etc.) (ENISA, 2017). Moreover, the network can be closed or open. The infrastructure of the IoT can be described in the same way as a classical Internet infrastructure (e.g. with gateways, routers, power supplies and security assets) (ENISA, 2017). Nowadays, an important network challenge is to find safe means to broaden bandwidth for the increasing volumes of big data transmissions generated by the significant number of connected IoT devices (e.g. the transition from 4G to 5G).

IoT devices or connected devices are pieces of equipment whose main capabilities are to transmit as well as receive data automatically. Consequently, all hardware, software, sensors, effectors or embedded systems able to exchange information with other devices without human intervention can be regarded as IoTs (Duffy, 2014; ITU-T, 2012; Ochs, 2017). The main characteristics of connected devices can be described as follows:

- Both physical and virtual (e.g. hardware, software, multimedia contents, applications, etc.) (ITU-T, 2012)
- Heterogeneous (as they are based on different hardware and software)
- Dynamic (able to change their communication patterns automatically)
- Identifiable and addressable objects
- Large-scale distribution problems (many IoTs are already physically and virtually obsolete. Many more are produced every day, causing security and logistics issues that are discussed in sections 4.1 and 4.2 of this TA) (Ajay Kumar Maurya and Ahmad, 2018).

In view of the evolution of technology, one could be forgiven for assuming that device memory and computing power were solely integrated so they can be hacked and used for criminal purposes, as demonstrated in section 5.1.

Big Data collection is also a relevant characteristic of the IoT because of the huge volume of data collected – and sent on to acquisition and processing centers — by device sensors. This points to the problem of confidentiality and data governance[7]. Moreover, powerful algorithms are needed for processing the data, and the relevant algorithms increasingly employ Artificial Intelligence (AI), especially when it comes to Deep Learning (e.g. Apple's Siri and Voice Over (Audio Software Engineering and Siri Speech Team, 2018)). It is therefore plausible that, in the future, the IoT will increasingly be linked to the AI field (Kersting and Meyer, 2018).

The IoT is a result of human society. From a holistic point of view, the IoT is a socio-political, security-related and economic phenomenon that needs to be addressed as such. This report examines the IoT from an ecosystemic point of view[8] — an approach that best explains the global and interconnected nature of the IoT (Colin and Verdier, 2012; ENISA, 2017; ICANN, 15:57:03 UTC; IoT Ecosystem, 2016). Moreover, an ecosystemic approach is optimally suited for highlighting the trans-socio-sectoral nature of the IoT.

Towards a holistic definition of the IoT ecosystem

This TA defines the Internet of Things and IoTs as follows: The IoT is a cyber-physical array of trans-sectoral pervasive network-ecosystems which consists of the interconnection via information and communication technologies of multiple connected devices and the data they share. An ecosystem is understood in this TA as a „*network of interactions among organisms, and between organisms and their environment*" (ICANN) (to encompass the societal, systemic and technical aspects of the IoT). The IoT is regarded as a trans-sectoral and societal phenomenon, as it is present in almost all aspects of daily life and affects all sectors of society (e.g. home automation, the health and entertainment industries, aerospace industry, critical infrastructures, defense industry, etc.).

[6] The terminology "the market" is understood here in its broadest sense as covering all the possible markets that are likely to produce IoTs.

[7] Due to lack of space and time, neither big data and data governance nor AI are addressed in this TA.

[8] For further information visit https://digital-ecosystems.org/

In this regard, IoTs are defined as all the physical and virtual connected devices which sense, compute and interact with each other without regular human intervention. Such intervention is usually needed, though, when the “self-management capabilities of the (IoT ecosystem) are exhausted” (Avsystem, 2019).

This broad and systemic conceptualization helps to conceptualize the IoT and IoTs in a dynamic way in which, for example, hybrid technologies such as smartphones, tablets or applications-based and software-based computers can also be understood as IoTs (Darwish et al., 2017; Openshaw et al., 2014; Piedad, n.d.; Stefanuk, 2017). Moreover, such an approach recognizes that IoTs can, depending on the system, also work together as an ecosystem in closed networks without any automated connection to the World Wide Web (www) or the Internet. This TA refers to these specific connected devices as closed-system IoTs. These are operational technologies (OT) and can be found in any complex closed network such as the Industrial Control systems (ICS) (Michel, 2017).

3 Why Is the IoT Hyped?

The definition above shows that almost every aspect of daily life is potentially affected by the IoT – from smartphones to lightbulbs, as illustrated in Figure 1 below. Moreover, the IoT raises the question of satellites, also considered to be IoTs. Satellites are critical infrastructures, however this issue is too often ignored (Stone, 2019).

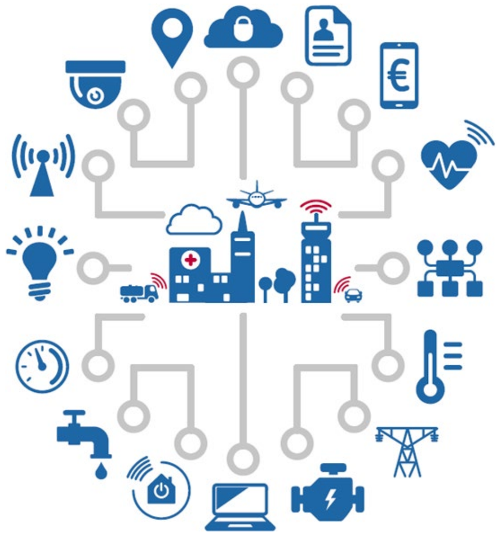

Figure 1: The pervasive IoT ecosystem (ENISA, 2017, p. 118)

Its ubiquitous nature and the fact that this is a relevant, rapidly developing field where technology advances exponentially, make the IoT very attractive for the overall economy (Gloria, 2016; Kleinhans, 2017). Consequently, IoT-related businesses are flourishing, for instance because the potential benefits the IoT brings to society represent an important additional business value (Openshaw et al., 2014). Moreover, research has shown that the IoT benefits almost all societal sectors, from entertainment to defense (Jungo, 2015; Kranz, 2018; Manyika et al., 2015; Ochs, 2017; Openshaw et al., 2014; Sicari et al., 2018; Slowey, 2017).

3.1 Societal benefits of the IoT

Five elements are crucial to create societal and economic benefits through the deployment of IoT devices:

Communications: The key benefit here is the ability to automatically communicate raw or computed information M2M or to people. IoTs can, for example, communicate the health status of a system’s components in real time and therefore provide the system administrator with meaningful insights or even prevent system malfunction or failure.

Big Data collection and analysis: IoT devices, by collecting and communicating an exponentially increasing amount of data, contribute to the building of

Big Data. The latter can improve the understanding of overall IoT ecosystems and therefore of customers' demands and behaviors (Ochs, 2017, p. 286).

Automation and control: The integration of IoTs into systems enables planned maintenance and management. Moreover, increased productivity and precision through supply-chain automation or self-learning and adaptive devices, software and applications potentially improve the precision and productivity of entire systems.

Security: When used in security-related ecosystems, IoTs can improve physical security for both humans and infrastructures (e.g. through video surveillance, access restrictions to hazardous locations and equipment, computer-assisted driving, data analysis, etc.) (Openshaw et al., 2014).

Increased revenue and cost savings: Each of the four above-mentioned categories, namely communications, Big Data collection and analysis, automation and control, and security can potentially increase revenue and save costs.

4 Why Is the IoT Insecure? Trends in IoT Economics

Due to the above-mentioned societal benefits of the IoT, the amount of connected devices has been increasing exponentially, with forecasts indicating that their number may reach 212 billion by 2020 (SGDSN, 2018, p. 28). This number raises serious concerns regarding the security and safety of the IoT because, according to academics and cybersecurity specialists, the great majority of IoT devices already connected to networks and integrated into our most sensitive systems (e.g. critical infrastructures) are there to stay, yet are poorly secured, infected, malfunctioning or obsolete; and this trend is rising, posing serious challenges to society (Bode, 2018; Chen et al., 2018; Dabbagh and Rayes, 2017; Lewis, 2016; Tonin, 2017).

One of the main reasons that have led to this situation is inherent to IoT economics because, as Lesley Carhart put it, "*In terms of security, things can be quick, cheap, secure, but not all three at once*" (Carhart, 2018). This logic is not exaggerated, especially considering that the IoT industry tends to invest in features which deliver a direct return on investment, while sacrificing security in the race to release products in time (Paratus People Limited, 2018). This economic trend is somewhat less pronounced in sensitive sectors like defense and critical infrastructures, though, where security standards are higher.

In order to better understand IoT economics and to highlight why the IoT challenges our society, this section first analyzes the trade-off between costs and security in IoT-related sectors. Second, it addresses the lack of awareness and knowledge as well as the information asymmetry regarding IoT security. Finally, this section looks into the design and lifecycle management of the IoT.

4.1 The vicious cycle of the IoT: a trade-off between costs and security

First of all, IoTs are ubiquitous and distributed in a very complex and rich ecosystem that involves humans, devices, networks and content. Moreover, the number of unsafe and unsecured IoTs "in the wild" has already reached a critical mass, which means that there is most probably no more turning back.

This critical mass represents a true societal challenge (economic, security and even ecological) because of the difficulties related to the logistics of the IoT: the replacement, updating or repair of IoT devices (physical or virtual).

Indeed, insecure design and poor lifecycle management make IoTs – physical or virtual – fragile, easily obsolete and extremely difficult to repair, update and replace. However, even where IoTs are replaceable, their rapid obsolescence increases the demand for the production of more IoTs, mostly with, unfortunately, poor security standards (Franceschi-Bicchierai, 2015a; Grebler, 2017).

This increased production causes the number of potential vulnerabilities distributed across networks to grow, thus widening the cybersecurity threat landscape further and further. Then, when the newly produced IoTs are compromised or have again become obsolete, they too need to be repaired or replaced, and so on.

This is a vicious cycle: Market pressure for more IoTs, created by short product lifetimes, drives the production of ever larger numbers of low-cost IoT devices. This cycle is illustrated in Figure 2.

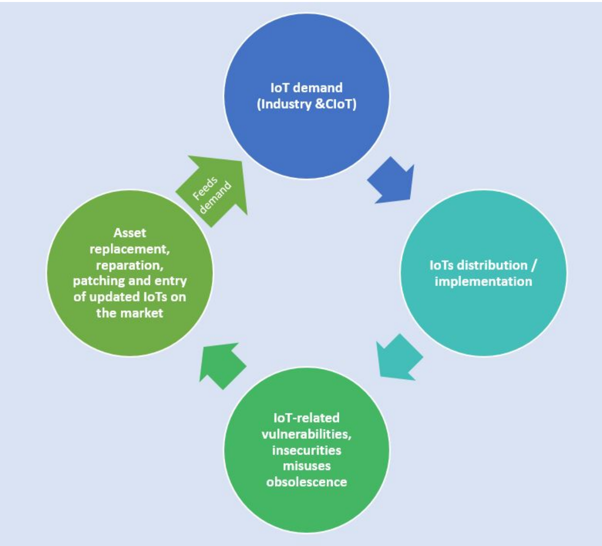

Figure 2: The vicious cycle of the IoT

From a technical point of view, the characteristics of IoT devices – and also Customer Internet of Things devices (CIoTs) – i.e. limited computing power and memory capabilities, hard coding, etc., challenge conventional security practices because producers and manufacturers all too often trade off security for lower production costs, ultimately giving rise to the above-mentioned vicious cycle (ENISA, 2017, p. 23).

Moreover, integrating security into IoTs can be difficult for many reasons: Above all, when it comes to integration and interoperability, stakeholders' different viewpoints and cybersecurity experience impact on the homogeneity and quality of IoTs security. Indeed, as of now, there are no clear international or national standards or regulations and therefore no clear liabilities when it comes to securing the IoT. Consequently, a large number of manufacturers focus more on usability and saving costs of production than on security.

As a consequence of the trade-off between costs and security, IoT-related vulnerabilities and challenges make it easier for cybercriminals to target or use IoTs, which have therefore become "easy prey" (Sattler, 2019). Computing devices which are poorly secured yet almost permanently connected to the internet provide criminals with a large number of devices as well as ample power and connection time. Moreover, the lack of security updates in IoT devices ensures that devices remain persistently connected to the net even if they are potentially infected.

Finally, a wide range of IoT devices are made by the same manufacturers, especially when it comes to CIoTs. Often manufacturers run different CIoTs under the same software, which makes it way easier for criminals to hack large numbers of devices using the same code (Kleinhans, 2017, pp. 9–11).

4.2 Lack of awareness and knowledge and information asymmetry

The fast-evolving nature of both cyberspace and the IoT, plus economic competition force companies to again and again come up with new products and release them sooner than their competitors (Paratus People Limited, 2018).

This forced march towards diversification and innovation raises the problem of the lack of awareness and knowledge regarding IoT security among both consumers and manufacturers.

First, the trend to produce this growing volume of IoTs or "smart devices" like smart washing machines, smart fridges or smart light bulbs is not a bad idea *per se*. The problem is that companies often lack the knowledge or/and the experience to build such items in a secure and sustainable way. This is often the case when established companies with no IT-related products expand into the IoT market. These companies are likely to externalize the security aspects of their products, often at a low cost. Moreover, IoT ecosystem-related business is new, and consequently security experts "*are more commonly familiar with 'business IT' security, but not with IoT security*"(ENISA, 2017, p. 54). Therefore, even if a company externalizes its products to IT security experts, it has little means to know if those experts are also IoT security experts.

Second, companies and consumers – when concerned about security and safety – tend to look at IoT devices in isolation from their ecosystems. However, contextualization is hugely imporant for understanding the specific threats affecting individual IoT ecosystems. For example, a connected house, a smart doll, smart pacemaker or smart industrial factory all expose devices, workers and consumers to different threats. Moreover, the possibility of cyberattacks differs between one ecosystem and another. As a result, awareness of ecosystems is crucial, and risks must therefore be analyzed systemically.

The third problem can be described as the "time factor": Without training and continuous education, employees cannot improve their knowledge and hygiene with regard to IT and IoT security.

Consequently, there is the risk that their knowledge quickly becomes outdated.

Fourth, IoT knowledge and awareness raise the question of the information asymmetry between consumers and manufacturers and the lack of economic incentives regarding investments in IoT security during the design and production processes.

When it comes to information asymmetry and the lack of economic incentives, academics face a chicken-and-egg problem: It is difficult to tell which came first, but it is easy to understand how one reinforces the other. Indeed, given the competitive nature of manufacturing, companies are not transparent about the firmware or source code of their products.

Finally, because of both the rapid evolution of the technology and the expertise it requires to test IoT devices, consumers, manufacturers and IT security companies and experts are unable to assess just how secure a connected device is at the moment of its release, nor after its implementation within an ecosystem. Consequently, this information asymmetry leads to scarce investments in the security of IoT devices and instead to a stronger focus on features that have a direct return on investment value, thus making it less attractive to invest in security (ENISA, 2017; Kleinhans, 2017).

4.3 Design, production process and lifecycle management

Several studies have shown that in most of the cases, when it comes to the design or development of IoT products, companies fail to have proper defense-in-depth strategies[9], security-by-design or privacy-by-design strategies[10], communication protections (for both internal and external interfaces), or strong authentication or authorization systems (ENISA, 2017, pp. 54–55). To what extent could a malfunctioning captor or actuator affect an oil platform, for example?

Moreover, the literature highlights that companies often fail to implement reasonable lifecycle management for IoTs, or to support security-by-design. Consequently, a wide range of IoTs quickly become obsolete and should be patched, updated or replaced in order not to turn into “easy prey” for malicious actors. However, given the above-mentioned poor lifecycle management, patching, updating or replacement is often difficult from a technical and economic viewpoint (too complicated and too expensive), especially in cases where companies go bankrupt and stop providing customer support, but their products are still in use (Chan, 2017; Grebler, 2017). Moreover, a deficiency in even one simple IoT device can cause an entire ecosystem to fail because the IoT comprises a broad variety of objects capable of endangering the entire supply chain if inadequately secured (Chan, 2017; ENISA, 2017).

This poor lifecycle management, especially concerning IoT security, is mostly caused by a phenomenon called negative externality. In a nutshell, this refers to the costs a third person has to pay because of a transaction between two other persons. (Economics Online, 2018; Kleinhans, 2017). Consequently, the security of IoT ecosystems can be seen as a negative externality nobody wants to pay for.

Finally, the above-mentioned points highlight that IoT security is often addressed in reaction to incidents rather than before they arise (ENISA, 2017, p. 55). This logic drives manufacturers to try to fix gaps in systems instead of making sure such gaps do not occur in the first place.

This systemic problem shows why the design and production phase of IoTs is decisive for security and safety. Low standards and an inadequate distribution of responsibilities within the economic sector highlight the need for stronger regulation and broader standardization in the field of the IoT.

4.4 Conclusion

With regard to the issue of overall IoT security and safety, the above brief analysis of the economics of the IoT points to a high degree of correlation between information asymmetry, a lack of knowledge, design and production processes, lifecycle management and a trade-off between costs and security. Together, these interrelated phenomena have created a fertile breeding ground for the complex, systemic societal challenge described above as the vicious economic cycle of the IoT. This in turn shows that economic laissez-faire regarding the IoT market is surely not the best solution to tackle IoT-related security and safety issues. Moreover, evidence suggests that the fundamental problem surrounding the IoT will not magically resolve itself over time but will instead necessitate comprehensive regulatory intervention and overall risk awareness.

[9] Defense-in-depth strategy first emanated from military strategy. It implies multiple layers of security controls surrounding an IoT device. (Son and Kim, 2012)

[10] Security or privacy-by-design with regard to IoTs means that the product has been designed from its conception to be secure and respect privacy.

5 How Is the IoT Insecure? Trends in IoT-Related Vulnerabilities

An increasing number of incidents using or targeting IoTs have been reported over the last 10 years. This can be explained by the sudden increase in the number of poorly secured and unsafe IoT devices in all societal sectors. Consequently, both black-hat and white-hat hackers have grasped opportunities provided by flaws in this new field to test and exploit system vulnerabilities.

This section discusses an IoT-related taxonomy of threats and an indicative timeline of prominent IoT-related cyber incidents.

5.1 Taxonomy of IoT-related threats and indicative timeline of prominent IoT security incidents and penetration testing

The most widely reported IoT-related incident was the Mirai Botnet DDoS attack. However, the IoT affords a much larger range of disruptive possibilities and threats, which are summarized as follows in this TA according to ENISA's "Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures"[11]:

- Nefarious activity / abuse: This category includes various DDoS attacks, malware, exploit kits, counterfeit by malicious devices (diverse hardware or software manipulations or the generation and use of rogue certificates), targeted attacks like Advanced Persistent Threats (APTs) or remote activity, modification of information through ultrasonic jamming / spoofing / cancelation or loss of information in the cloud and attacks on privacy (abuse of personal data, authorization or identity, social engineering or compromising confidential information like phishing, untrusted links, etc.)
- Outages: this category includes various failures like system, device and hardware failures, loss of support services and network outages
- Physical attacks including device modification or destruction (sabotage)
- Disasters: When perpetrated on critical infrastructures, attacks can result in disasters like floods, fires or various exposures
- Damage or loss of IT assets like sensitive data leakage
- Eavesdropping, interception and hacking: This category includes network reconnaissance, information gathering, session hijacking, replay of messages, man in the middle, IoT communication protocol hijacking and the overall interception of information, e.g. by rogue hardware or software interception
- Failures and malfunctions: software vulnerabilities (configuration errors, software bugs, weak authentication or cryptography) and failures by third parties like internal service providers, cloud service providers, remote maintenance providers and security testing companies (ENISA, 2017, p. 32)

Most of the attacks aimed at IoT devices or using them as vehicles are the result of poorly secured IoT ecosystems which have become compromised.

In order to further our understanding of the disruptive potential of IoTs and how they challenge society, Table 1 sets out a timeline of prominent IoT-related incidents to highlight trends regarding the overall *modus operandi*, main propagation vectors, aims and nature of alleged or identified perpetrators.

We have grouped alleged or identified perpetrators into three categories based on their backgrounds: Cybercrime actors (C), Nation State actors (NS) and Penetration Testing actors (PT). The problem of technical and public attribution related to the nation state and criminal categories is not be addressed here.

Additionally, Table 1 makes a distinction between attacks where IoT devices were used as vehicles (means), and attacks directly aimed at IoT devices. The table also lists prominent cyberattacks that unintentionally affected IoT ecosystems or IoT devices – connected to the Internet or in closed networks – because some of the major IoT-related attacks were embedded into wider IT attacks.

[11] The taxonomy of threats in this TA is based on the ENISA taxonomy because ENISA's work adopted an ecosystemic approach to the IoT. Similar to ENISA, this TA is also based on an ecosystemic definition and conceptualization of the IoT, and ENISA's approach to IoT-related threats is therefore well suited for this TA.

Table 1: Indicative timeline of prominent IoT-related security incidents and penetration testing

Date	Incident	Description	Main Threat Vectors	Type	IoT as means or target
2009-2011	Stuxnet aimed at an Iranian nuclear plant's SCADA systems	Stuxnet is "*a worm using four zero-day exploits vulnerabilities and infecting computer networks through USB flash drives*" that targeted SCADA systems (Baezner and Robin, 2017, p. 4).	Malware, exploit kit and device sabotage via USB ports, routers and Siemens Simatic SCADA systems.	Alleged NS	Target
2009	Puerto Rican smart meters hacked	Insider attack conducted by former employees aiming to reduce power bills.	IoT communication protocol hijacking & interception of information: The hackers used an optical converter device connecting laptops and smart meters. The use of strong magnets is also suspected (Ireland, 2001).	C	Target
10.08.2013	Foscam IP baby-cam hijacking	The hackers were able to spy (audio & video) and to communicate with kids and parents through the microphone-speaker systems of cameras.	IoT communication protocol hijacking & attacks on privacy: Poor default password easily hackable with a password-cracking program let attackers take control over the cameras (Vaas, 2015).	C	Target
15.11.2013-15.12.2013	Target Data Breach	Private data from over 70 million customers stolen.	Phishing with Zeus & Exploit at point-of-sale systems (IoTs) & network reconnaissance (Radichel, 2014)	C	Means
2011-2014	Accessing of the climb command of Airbus and Boeing airplanes	Chris Roberts claims he could access 20 airplanes' climb commands through their inflight entertainment systems. The FBI has not confirmed this (Barrera, 2015).	Climb Command hijacking through inflight entertainment systems penetration	PT	Target
01.2015	BMW's Connected Drive vulnerabilities demonstration	Researchers sent remote unlocking instructions to vehicles by imitating BMW servers (Paganini, 2016a).	Counterfeit by malicious devices	PT	Target
21.07.2015	Jeep car remotely hijacked for demonstration	Charlie Miller and Chris Valsek demonstrated how to gain full control over the car remotely.	Exploit via a vulnerability in the vehicle's Internet-connected entertainment system (Rachid, 2018)	PT	Target
29.07.2015	Tracking Point's smart sniper rifle hack demonstration	Runa Sandvik and Michael Auger exploited vulnerabilities in the rifle's software.	Exploit & session hijacking via the poorly secured Wi-Fi connection of the rifle's targeting system (Williams, 2015)	PT	Target
08.11.2015	VTech's Learning Lodge app servers	The breach affected VTech's servers through its cloud, which was connecting the smart toys (IoTs) to various services. The hacker collected pictures, full names and addresses of 6.4 million children and 4.9 million adults. Here, the target was an online app (virtual IoT). Physical IoTs were used as a vehicle to collect private data.	Attacks on privacy & Man in the middle & Network reconnaissance & IoT communication protocol hijacking via the company's poorly secured servers (Franceschi-Bicchierai, 2015)	C	Means
01.11.2016	PanelShock Exploit on Schneider Electric	This exploit could remotely freeze Human Machine Interface (HMI) panels and disconnect them from the SCADA network. SCADA systems (IoTs) were targeted but human intervention was necessary to reach them.	Exploit & software vulnerabilities & failure of devices via the constructor's poorly secured Web Gate web service, then spreading malware via poorly secured IoTs (Paganini, 2016b)	PT	Target
19.09.2016	Mirai - DDoS on OVH hosting provider	Peak of traffic: 1 terabyte per second (TBPS) powered by 152,000 hacked IoT devices	After spoofing, Mirai spread into poorly secured IoTs (default access credentials) turned into botnets by using malware (Bonderud, 2018; Segal, 2016).	C	Means & target
20.09.2016	Mirai - DDoS on "Krebs on Security" website	Peak of traffic: 620 gigabytes per second (GBPS)	*Idem.* (Bonderud, 2018; Segal, 2016)	C	Means & Target
15.09.2016	Hajime P2P botnet	Vigilante IoT worm that blocked rival botnets (including Mirai) and built a peer-to -peer (P2P) botnet. More than 300,000 IoTs infected in April 201l7.	Uses same IoT vectors as Mirai on OVH (Kaspersky Lab, 2017)	C	Means & Target
21.09.2016	Mirai- DDoS on Dyn DNS provider	Blocked access to several popular websites like Netflix, Twitter, PayPal and Amazon. Peak of traffic: 1.2 TBPS.	Same vectors as Mirai on OVH and Krebs.	C	Means & Target

Date	Incident	Description	Main Threat Vectors	Type	IoT as means or target
03.11.2016	DDoS on Valtia building blocks' central heating system	Malfunction in Valtia's central heating and hot water systems. This DDoS attacks happened in Finland and was likely using the Mirai botnet.	DDoS attack on poorly secured IoT components (Daws, 2016)	C	Means & Target
27.11.2016	Mirai DDoS on Deutsche Telekom Network	500,000 infected IoTs. 900,000 customers affected.	Like other Mirai attacks, via Deutsche Telekom's vulnerable IoTs, incl. routers, DVRs and cameras (Kan, 2016)	C	Means & Target
25.12.2016-08.01.2017	Cloudpets' DB held for ransom	Cloudpets IoT Toys compromised because of the eavesdropping on 820,000 accounts.	Vectors are both IoT and non-IoT: vulnerability created on IoTs by eavesdropping (Franceschi-Bicchierai, 2017b)	C	Target
17.02.2017-27.02.2017	Cloudpets and "Meine Freundin Cayla" – unsecured Bluetooth	Vulnerability concerning all Cloudpets. Anyone with a smartphone within a range of 10 m was able to upload and receive audio.	IoT communication protocol hijacking & attacks on privacy via IoTs Bluetooth and via the above-mentioned eavesdropping (Franceschi-Bicchierai, 2017b)	C	Target
20.03.2017	BrickerBot	Around 10 million contaminated IoTs. Bot designed to permanently incapacitate poorly secured IoT devices.	Device destruction & device modification of poorly secured IoTs (Shah, 2017)	C	Target
04.05.2017	Trend Micro and POLIMI demonstration on industrial robotic systems	Trend Micro and the Italian technical university Politecnico di Milano (POLIMI) exposed the vulnerability of 83,000 industrial robotic units.	Device modification via IoTs' weak authentication, cryptography or outdated software (Trend Micro, 2017)	PT	Target
29.08.2017	Recall of 465,000 Abbott pacemakers	US Food & Drug Administration issued a letter for the voluntary recall of the pacemakers for safety reasons due to potential hacking discovered by MedSec cybersecurity firm.	Device modification via outdated firmware and security protocols (Security Today, 2017)	PT	Target
28.01.2018	Strava reveal location of military based and personnel	Strava, a fitness-tracking company accidentally revealed on its website over 1 billion activities including 13 trillion GPS data points, and in so doing revealed sensitive location and personnel data.	Network reconnaissance and attacks on privacy via poor classification and protection of GPS and user data (Novak, 2018)	-	Means
08.2018-10.2018	GhostDNS botnet campaign aimed at Brazilian Bank	Some 100,000 routers compromised in Brazil. Attack aimed at customers' bank credentials.	Counterfeit by malicious devices & attacks on privacy via poorly secured routers turned into botnets (IoT Security Watch, 2018)	C	Means
19.09.2018	Avast and VessOnSecutiy discovers Torii DDoS Botnet	According to Avast, Torii is a Mirai-like botnet but far more sophisticated.	Infection vectors similar to Mirai attacks (Sattler, 2019)	C	Means

5.2 Conclusion

All of these attacks demonstrate the massive potential of IoTs to cause disruption and even destruction over a relatively short term. Moreover, this list identifies the possibilities and possible effects of realistic IoT-related attacks.

Indeed, attacks like the ones presented in Table 1 indicate that attackers successfully took control of IoT devices or used them as vehicles to reach their goals. Table 1 also shows that IoT devices are sometimes accidentally involved in data leakage or malfunctions. Moreover, the Trend Micro and POLIMI demonstration on industrial robotic systems, Stuxnet and the PanelShock exploit elevate the problem to another level because of the importance of the IoT devices involved and the dangerousness of these attacks / penetration tests. In the one incident, industrial robots were hacked, and in the other PanelShock and Stuxnet successfully penetrated SCADA systems (Operational Technology[12]). This indicates that the IoT is not only potentially insecure, but also unsafe, especially when it comes, for example, to industrial systems, hacked cars or pacemakers.

Moreover, Mirai and Torii attacks highlighted the alarming number and ubiquitous nature of insecure, poorly protected and unpatched IoT devices running throughout the world. These attacks prove that almost any connected device can be used as an entry point for cyberattacks. In addition, all of these incidents highlight the highly diverse nature of attacks: malware, remote control or DDoS attacks using IoT-botnets etc. The Mirai DDoS attack on the Deutsche Telekom Network, for

[12] "*Operational Technology (OT) refers to computing systems that are used to manage industrial operations as opposed to administrative operations*" and are complementary to Information Technology (IT) and Customer Technology (CT) (Williamson, 2015).

example, could have caused large parts of Europe's Internet to fail, had it been completely successful.

Furthermore, Table 1 points to an overall trend in the *modus operandi* of attacks: A majority of them consist in combined attacks involving more than one medium and exploiting more than one vulnerability in the targeted systems. Moreover, IoT-related attacks are often part of broader cyberattacks or goals. In this regard, similar to their non-IoT-related counterparts, these attacks use IoT devices and their networks both as means and as targets in order to pursue criminal or strategic goals.

Table 1 also suggests that a large majority of IoT-related cyberattacks are perpetrated for criminal motives. The other main trend in IoT-related attacks is penetration testing. With regard to the IoT, only Stuxnet allegedly originated from nation state actors. However, as in non-IoT-related cyberattacks, the question of attribution remains complicated. This trend has also been observed in cyberattacks where IoTs are not involved.

Table 1 further shows that the actors involved in IoT-related attacks are a good indicator of the overall tendency towards highly complex tools being used to attack IoT ecosystems. It appears that criminally motivated attacks tend to use less complex or more redundant attacks, whereas state actors or penetration testing tend to use far more elaborated exploits. This trend, which has also been observed in cyberattacks where IoT devices are not involved, can be explained by the wide range of cheap malware available on the deep web.

Finally, the nature of these attacks shows that IoTs, when misused, also constitute a threat to data privacy (e.g. baby-cams, smart watches, Cloudpets, Strava, etc.). Indeed, when it comes to wearable IoT devices or any sensors collecting information, the resulting data can be misused for criminal purposes, where data can be sold, stored and analyzed later on.

This look at IoT-related attacks suggests that, as long as IoT devices are unsecured or poorly secured, the number of attacks is likely to grow in line with the increasing number of IoT devices entering the market and landing in the public or private sector. Moreover, the potential consequences of attacks are very serious, wide-ranging and potentially disruptive because of both the number of IoTs in circulation and their sensitive role in complex systems (e.g. ICS)(Amyx, 2014).

6 The Regulation of the IoT: A Long Haul

This section provides a general overview of the significant evolution and debates in regard to IoT-related governmental and international regulation and its strategic implications. To do so, this section first empirically analyzes the occurrences of the terms "IoT", "Internet of Things" and "internet of things" in national cybersecurity and cyberdefense strategy documents to determine which countries address the IoT in their cybersecurity strategies. Second, it summarizes major government bills and recommendations regarding IoT regulation to explore the IoT-related governmental landscape. Third, this section addresses the contributions of major international organizations to IoT regulation. However, an empirical analysis is difficult in this context due to time and space constraints as well as insufficient transparency and homogeneity of the sources and literature regarding international organizations and the IoT. Fourth, this section summarizes the major topics addressed by both governments and international organizations with regard to IoT regulation. Finally, it discusses the implications of IoT regulation in regard to the defense sector and the armed forces.

6.1 Governments and IoT regulation

Word search

A word search was performed on government documents for the following words and phrases, using the MAXWDA word search analysis program: "IoT", "Internet of Things", and "internet of things". These three terms were chosen because they are widely used in the literature on IoT-related topics. However, "IoT" is, of course, also used as an acronym for both of the other terms. This empirical analysis was performed to determine which states use these terms in their respective cyber strategies. Assuming that strategy, politics and regulation are interconnected, the mention of these terms in national strategy documents is interpreted in this TA as a sign that the respective country regards the IoT as a security priority and therefore has the IoT on its national policy radar. This in turn is interpreted as a call for further regulation in the IoT domain.

According to the ITU National Strategy Repository, as of 2019, 124 of the 194 ITU Member States (including the State of Palestine) have a national cybersecurity strategy or are in the process of developing one (ITU, 2019), and 110 relevant documents are available in English.

The word search, inspired by Baezner and Robin's Trend Analysis on Cyber Sovereignty and Data Sovereignty (2018), was executed on 89 different countries' cybersecurity and cyberdefense strategies, for a total of 123 documents. All materials used in this section are unclassified and available in English. The word search for this TA did not include countries without national cybersecurity strategy, in the process of developing a strategy or without an English and / or publicly available version of its strategy.

Out of 110 countries scanned for this analysis, only 20 had developed cyberdefense or cybersecurity strategies containing the precise wording. The great majority of them are European countries: United Kingdom, Netherlands, Montenegro, Denmark, Macedonia, Austria, Croatia, Czech Republic, Denmark, Luxembourg, Switzerland and Italy. Asia-Pacific countries also use the abovementioned wording: Taiwan, Singapore, Japan and Australia. Finally, the American continent is represented by Jamaica and Canada, while the African continent is represented by Senegal and the United Arab Emirates.

The word search indicates that the states using these terms in their strategies are mostly Western countries, which are also overrepresented in this analysis. However, the literature also shows that incentives for further regulation of the IoT have emanated from western countries, which are thus more likely to write about the IoT in their national cybersecurity strategies.

This TA assumes that the use of one or all of the above-mentioned terms suggests a certain, even minimal, degree of awareness in regard to the IoT. However, an absence of these terms in some strategies does not conversely mean that the respective countries do not tackle the problem of IoT security in other documents or bills. As an example, the cybersecurity strategies of both China and the USA were negative to this test, while the literature indicates that both of these countries are active in regard to IoT-related activities.

The frequency of use of these terms in relation to the strategies' years of publication highlights a number of interesting facts: Most of the countries cite IoT-related terms fewer than 5 times with an overall average of 2.0 times, regardless of the year of publication (Denmark, Macedonia, Austria, Australia, Croatia, Czech Republic, Canada, Luxembourg, Switzerland, Singapore, Senegal and Italy). Montenegro, the United Arab Emirates and Jamaica cite IoT-related terms 5 times, and the United Kingdom and Netherlands 8 and 9 times respectively. Finally, Taiwan cites IoT-related terms 27 times and Japan 95 times.

Section 2.1 above shows that the first occurrence of "IoT" or "Internet of Things" goes back to 2005. However, the oldest cybersecurity or cyberdefense strategies citing these terms date back to 2013 (Austria, Italy, Japan and the Netherlands). The most recent strategies referring to the IoT were issued in 2018 by Canada, Switzerland, Luxembourg and Macedonia. The express mention of the IoT in strategies is likely to be in response to the rapid increase in IoT-related cyberattacks from 2013 onwards.

The word search indicates that countries first started to use IoT-related terminologies in their strategies in 2013, as the first wave of IoT-related incidents and penetration testing began. However, these early strategies only referred to IoT-related terms infrequently (up to 5 times).

The IoT trend began to take off with the second wave of attacks, in around 2016. Consequently, the strategies which cite IoT-related terms most frequently were released between 2016 and 2017. This tendency can be understood as a reaction to the increasing number and intensity of IoT-related incidents (e.g. Mirai attacks). It is also noteworthy that the countries whose strategies refer most frequently to IoT-related terms are Japan and Taiwan. This is no coincidence if we contextualize these two countries: They are both industrialized countries with consumers, both industrial and individual, who use gadgets and IoT devices more extensively than their counterparts in Western or African countries. Moreover, in the case of Japan, it is reasonable to assume that there is a correlation between the development of the country's cybersecurity and IoT-related security strategy and the fact that it will host the 2020 Olympic Games. In this context, the Japanese National Institute of Information and Communications Technology (NICT) engages deeply with cybersecurity – and therefore IoT security – at Big Events through, among others, surveys aimed at checking potential vulnerabilities in objects such as routers, webcams and web-connected home appliances (AFP, 2019).

Finally – and this is a generally observed trend – states have become more likely to include or expand on IoT-related topics in revisions or updates of their strategies.

The word search results also point to the increasing use of IoT-related terms in national cybersecurity and cyberdefense strategies. This may indicate increased awareness of the subject, but further contextual and qualitative research will be required to elucidate the extent to which this is true. However, the word search conducted for this TA highlights a tendency towards a proportional increase in the development of cybersecurity strategies, including IoT-related terms, relative to IoT-related cyberattacks. This increase of IoT-related terminology can be interpreted as a strategic call towards the further conceptualization and regulation of the field.

The correlation between poor IoT conceptualization in states' cybersecurity or cyberdefense strategies and low average frequencies of corresponding terminology, and *vice versa*, is plausible in most cases. However, even if some countries, like the USA or China, do not refer to the IoT at all in their cyber strategies, they do tackle IoT-related topics in national or state bills, recommendations, codes of practice, etc., and some of them have already introduced concrete guidelines in recent years. The best examples are the USA, the state of California and the UK.

National policies

On 27.01.2015, the USA Federal Trade Commission (FTC) released a detailed report on the IoT titled "Internet of Things: Privacy & Security in a Connected World". This report emphasizes data privacy and the benefits and security risks of the IoT, and makes several recommendations, including one to implement "security by design" (FTC, 2015a, 2015b). In September 2017, the US Senate introduced a new bill, which has not yet passed Congress, called the "Internet of Things Cybersecurity Improvement Act of 2017". This bill is less oriented towards manufacturers and more towards government. Once it becomes law, it will require government agencies to include clauses in their IoT-related agreements that allow them to demand security features in IoT systems acquired by the USA government.

On 28.09.2017, the Governor of California, Jerry Brown, approved bill SB-327 "Information privacy: connected devices". This is the first known bill to be signed which is directly related to the IoT. The law, which will enter into force on 01.01.2020, is aimed at regulating IoT security and privacy directly at the manufacturer level (State of California, 2018). It defines IoT-related terminology and sets out the way manufacturers are required to behave when it comes to IoT security. However, the document does not define security terminology exhaustively; a fact which considerably hampers its security and safety-related regulation potential (State of California, 2018).

On 28.02.2019, the UK Department for Digital, Culture, Media and Sport (DCMS) published its collection "Secure by Design", which it describes as the "Government's Code of Practice for Consumer Internet of Things (IoT) Security for manufacturers, with guidance for consumers on smart devices at home" (DCMS, 2019). This collection contains the following set of guidelines aimed at making the entire IoT ecosystem safer:

- Code of Practice for Consumer IoT Security, released on 14.10.2018
- Code of Practice for Consumer IoT Security – international versions, released on 14.10.2018
- Mapping of IoT security recommendations, guidance and standards, released on 14.10.2018
- ETSI industry standard based on the Code of Practice, released on 04.03.2019

This is the most notable regulation measure regarding the IoT ecosystem so far adopted. The collection of guidelines aims to improve security, safety, protection and good practices throughout the IoT ecosystem by involving both consumers and market actors. However, at no time was this collection of guidelines intended to be legally binding or mandatory. As a consequence, companies, manufacturers and consumers are given the choice to apply it on a voluntary basis.

This formula is, nevertheless innovative regarding the field of IoT regulation and would, if broadly implemented, fill in the knowledge gap both consumers and manufacturers are experiencing with regard to IoT security and safety. Moreover, some influential UK manufacturers have already adopted the Code (Ashford, 2018; Inside Privacy, 2018).

6.2 International organizations and IoT regulation

When it comes to IoT-related regulation, it seems that international organizations and governments have finally realized that IoT security is a serious concern.

As early as in 2004, NATO started to standardize and normalize military IoT-related technologies within the framework of its Standardization Agreement (NATO STANAG) when it standardized RFID technology (NATO STANAG No. 2233). At the time, the concept of the IoT was still at a very early stage. Most recently, NATO agreed to list further RFID and GPS asset-tracking technologies in the NATO STANAG (Swedberg, 2019).

In 2016, NATO's Information Systems Collaborative Support Office (CSO) started a three-year study on the IoT and, in 2018, it decided to continue a two-year program on "Munition Health Management Technologies". The CSO study emphasizes data management, sensors, inventory monitoring, missiles and torpedoes, passive RFID, performance-based acquisition, propulsion & power systems and stockpile pooling (STO, 2019).

NATO has published only one document that clearly defines and conceptualizes the IoT. This document, "The Internet of Things: Promises and Perils of a Disruptive Technology", also addresses the need to secure critical infrastructures and defense-related IoT assets (Tonin, 2017).

In 2005, the ITU published its first report on "The Internet of Things". That document constitutes the earliest research paper to address the conceptualization and definition of the IoT from a societal, security and safety perspective. In so doing, the research addressed IoT-enabling technologies, IoT market potentials and the most critical challenges in this domain (ITU, 2005). The document was not only revolutionary at the time, but also inspired many international organizations, governments and civil society organizations to address the issue of the IoT. After 2005, the ITU launched a process of discussions, studies and reports to address IoT standardization under the heading of "Global standards for the Internet of Things" (ITU-T, n.d.).

On 14.05.2016, the European Union (EU) Parliament approved the General Data Protection Regulation (GDPR), which was implemented as of 25.06.2018. In a nutshell, this regulation aims to reinforce data privacy and the protection of personal data by unifying relevant regulations within the EU. With its "privacy by design" provisions, the GDPR requires data privacy and security to be considered at the early product development stage. The GDPR applies to all persons and companies within the EU and the European Economic Area (EEA).

However, when addressing the IoT, the GDPR is vague and limited: Only the sections referring to *"large-scale processing operations"* could be interpreted as an attempt to target the IoT ecosystem in relation to data privacy (EU Council, 2016, no. 91).

More precisely, when it comes to automated data processing – which is typical for IoT systems – the GDPR requires users to give consent before big data may be analyzed. However, this consent would be difficult to obtain for each instance where sensors collect data, contrary to GDPR requirements (EU Council, 2016, nos. 90–96).

In September 2017, the European Parliament issued a regulation titled "Cybersecurity Package", which addressed IoT technology. In November 2017, ENISA proposed a comprehensive study conceptualizing and defining the IoT ecosystem together with its vulnerabilities and challenges (security, safety and data privacy), and issued a number of guidelines (ENISA, 2017; European Commission, 2017).

In August 2018, the International Organization for Standardization (ISO) launched the ISO/IEC JTC "Internet of Things and related technologies", which is concerned with the definition and conceptualization of the IoT, the IoT reference model and architecture, and with what ISO refers to as "IoT trustworthiness" – emphasizing IoT safety, security (IoT system Information Security Management System and IoT system & product Security Life Cycle Reference Model), privacy and data protection, reliability and resilience (ISO, 2018). In February 2019, ISO/IEC published the document series "Internet of things (IoT) – Interoperability for internet of things systems", which focuses on interoperability within the IoT ecosystem (ISO, 2019).

Even the United Nations (UN) joined the IoT trend in 2018, when they questioned IoT standards and security from a business perspective through a conference organized by the UN Centre for Trade Facilitation and E-business (UN/CEFACT).

6.3 Conclusion

This section highlights the most notable contributions governments and international organizations have made so far to the earliest stages of regulation – and thus security and safety – of the IoT ecosystem. The intent of the aforementioned initiatives and their potential effects can be summarized as follows (Kleinhans, 2017):

- **Increased liability and market transparency in terms of technical standards for IoT devices**. This would reduce the information asymmetry between consumers (both governmental and civilian) and the industry with the goal to increase trust-building between stakeholders. It would also provide an incentive for industries to further regulate the IoT ecosystem and improve its security standards (minimal standards, security by design, data security and IoT ecosystem lifecycle management).
- **Market surveillance**. Responsive market surveillance could encourage manufacturers' compliance and good conduct with regard to securing IoT products.
- **Standardized certification organizations and multi-level security assessments**. If security standards are proportional to the associated potential for physical or societal harm, price, lifetime, etc., then security standards and behaviors could consequently be improved as a result.
- **Privacy and data governance.**

These points are critical when it comes to achieving higher security standards regarding the IoT ecosystem. If implemented, they could finally result in breaking the vicious IoT cycle described in section 4.1.

However, while work has been done regarding IoT regulation, none of the relevant initiatives are mandatory or coercive. Instead of insisting on mandatory security standards, governments and international organizations seem to prefer a softer approach consisting of expanding economic incentives for manufacturers to adopt higher security standards. This approach has the advantage of giving the IoT economy a certain amount of time to adapt. At the same time, it seems to entail a long haul because of the dichotomous dynamic related to IoT economics. The situation resembles two powerful actors pulling on the two opposite ends of a rope: One is profit, the other is security/safety, and the rope is the associated negative externalities.

7 Defense Sector: Addressing IoT Ecosystem Challenges

All the above-mentioned IoT-related dynamics and challenges certainly have an impact on the defense sector as well as on its means and capabilities.

In order to better understand the ongoing dynamics and implications of the IoT ecosystem in relation to this peculiar domain, this section first highlights how the defense sector benefits from the IoT technology and ecosystem. It then outlines how IoT-related vulnerabilities can affect the defense sector. Finally, this section briefly explores regulatory aspects of the IoT in relation to the defense sector.

7.1 Benefits of the IoT in the defense sector

With regard to the defense sector, the IoT can be analyzed analogously, even if this domain has specific needs such as higher security and safety standards and more stringent confidentiality policies. On the positive end, IoT usage can lead to increased efficiency, wider automation, reduced human error and costs through automation and the increased collection and analysis of data (Arashi et al., 2017; DefenceWorld.net, 2018; Gloria, 2016; Tapestry Solutions, 2017; Tonin, 2017a; Zheng et al., 2015).

For example, the Chinese People's Liberation Army (PLA) provided combat soldiers with smart watches to collect and analyze data. These watches are currently being tested by individual PLA Navy soldiers, and they have already proven useful. According to official press releases, "*the smart watches are equipped with verification systems, electronic compasses, BeiDou satellite navigation and other remote receivers*"..., and their use has resulted in a ..."*marked reduction in the time it takes to locate and extract an injured soldier*" (DefenceWorld.net, 2018).

The defense sectors where IoT technologies are most prevalent are: communications (e.g. RFID, GPS, etc.), electronic & cyberwarfare and intelligence (e.g. strategic use, Big Data collection), vehicle safety (e.g. sensors and automation), and healthcare and supply (sensors and automation). Indeed, in each of these sectors, processes can be automated or enhanced through the IoT (Tonin, 2017b, p. 10). For example, the USA has already incorporated IoT technologies in the four following areas: sensors, fire control systems, mobile technologies and logistics management (Tonin, 2017, p. 9).

7.2 Trends in IoT-related vulnerabilities and the defense sector

As shown above, the IoT can benefit the defense sector. However, Table 1 illustrates that IoT-related cyberattacks are quite disruptive and can therefore drastically impact on the environment (SASE), freedom of movement (FoM) and, more generally, on the proper conduct of military operations, in particular joint operations, because of the involvement of multiple military branches.

Communications, electronic and cyberwarfare, intelligence, healthcare, vehicle safety and supply are the most exposed branches because of their likely use of IoT devices in their defense systems and networks. As a result, IoT-related cyberattacks on these sectors can have the following effects: DDoS, physical damage, loss of production, malfunction and accidents, loss of communications, physical network damage, information leakage, panic and loss of confidence in the army or the chain of command (Arashi et al., 2017; Tonin, 2017, p. 10).

The most infamous known incidents in this regard are the Strava case, the TrackingPoint TP 750 rifle penetration test (while this rifle is generally not used in the military, its PT shows the risks related to IoT rifles) and the SZ DJI drone vulnerabilities. These three different attacks highlight the landscape of IoT-related threats in the defense sector.

Indeed, the Strava case revealed classified locations of the USA Armed Forces and enabled some to attribute GPS positions to individuals' personal data (Novak, 2018). This represents tremendous potential for data leakage, spying and, even worse, virtual or physical targeting.

Data leakage or spying concerns also arose in an incident regarding a different military IoT technology, the DJI phantom 4 drone. Indeed, after various vulnerabilities were identified, presumptions of possible Chinese spying and data leakage were raised. The issue was consequently addressed by the USA and Australian Armed Forces, which imposed a ban on the above-mentioned drones (Kilbride and Xiao, 2018).

Moreover, when Runa Sandvik and Michael Auger exploited vulnerabilities in the TrackingPoint TP 750 rifle software, they highlighted how easy and dangerous the pairing of guns and the IoT can be when not properly secured. Indeed, they were not only able to make the shooter miss a target, but they also successfully programmed the rifle to aim and shoot at a completely different target (without the shooter even noticing) (Williams, 2015). This kind of incident would have extremely serious implications if similar vulnerabilities were found on larger weapons systems.

A good example of larger weapons systems are semi-autonomous armored vehicles, which can nowadays be equipped with IoT devices. For example, the Swiss-made fully-armored, remotely operated mine-clearing device DTR Digger D-3 (GPS-enabled) is currently being deployed, mostly on the African continent (GICHD, 2013; Military-Today, n.d.). According to open-source material, no cyber-related vulnerabilities have been reported referring to this model yet, but this does not mean that such systems are vulnerability-free.

Russia took automated vehicles to another level with the Kalashnikov Uran-9, which is equipped with "*anti-tank missiles, an automatic cannon, and a machine gun. It can also be reconfigured to carry different weapons like surface-to-air missiles. Additionally, the unmanned vehicle is equipped with advanced optics and targeting systems including a laser warning system and thermal imaging*" (Chow, 2018). This armored vehicle has been deployed, even though it suffers from critical deficiencies like "*periodic cases of both short-term and long-term loss of control; inconsistencies within the targeting software and hardware; and operational delays in actually firing the vehicle's intimidating weaponry*" (Keller, 2019). These examples – and others like drones, airplanes, ships, etc.— are concerning because there is no guarantee these machines will not be compromised in the future to the extent that they rely on IoT systems. If they become compromised, this would constitute a serious threat to both civilians and soldiers.

The above is just a short list of examples to highlight why the defense sector can expect to be increasingly affected by the IoT trend. Indeed, the armed forces and defense industry – just like other sectors of society – are deploying an increasing number of IoT devices and systems, some of which are not fully developed or poorly secured. This increases the risks of cyberattacks on and malfunctions of devices of strategic value and lethal potential.

7.3 Regulatory aspects of the IoT in relation to the defense sector

As seen above, most of the national cyberdefense and cybersecurity strategies are just beginning to consider the security and safety implications of the IoT ecosystem. Moreover, from a legal point of view, cybersecurity and therefore IoT-related security in the defense sector fall under the state's prerogative and are thus subject to government legislation.

The first challenge in this context is closely linked to relevant infrastructures. Indeed, the main assets of the defense sector which require protection are critical infrastructures and national defense assets. While IoTs directly linked to sensitive domains are easier to control, the defense sector also needs to consider CIoTs, whose number is growing exponentially and which form part of ecosystems that are increasingly interconnected with critical infrastructures.

However, the room for maneuver when it comes to cost-benefit vs security considerations is only small, even if supply chain security is not always easy to control.

The second challenge is the difficulty to manage government authority and the accessibility of IoT devices that are frequently deeply embedded in national economic infrastructures, owned by private individuals and companies, or possibly even located in other countries (Arashi et al., 2017).

Thus, when it comes to the defense sector, regulation should be stepped up over the civilian sector by legally prescribing more stringent IoT security and safety standards. Indeed, while the CIoT and the OT sectors may be able to get away with a certain *laissez-faire*, as seen above, the defense sector certainly cannot afford to indulge in such a trade-off.

Finally, when it comes to military strategy, another dilemma arises at a more fundamental level, namely Freedom of Movement (FoM) and strategic advantage as classically examined by Carl von Clausewitz (2008). Put in a nutshell, excessive homogeneity (regulation and standardization) leads to a high degree of predictability and consequently reduces both strategic advantage and FoM, and this also applies to the greater complexity and vulnerability resulting from the logic dictated by the IoT. However, in our interconnected world, where defense cooperation is highly important and often inevitable, a minimal degree of homogeneity is needed to ensure the interoperability of armed forces systems. The broad benefits of this doctrinal and technological compatibility are exemplified by NATO's joint operations, where interoperability cannot be guaranteed without technical NATO standards (NATO STANAG). This, however, raises the issue of the optimal balance between regulation and strategic advantage, and this dilemma makes no exception for the IoT ecosystem.

8 Conclusion and Further Considerations

This Trend Analysis provides practitioners and researchers in the field of cyberdefense and cybersecurity with means to contextualize and conceptualize the IoT from a socio-political perspective, and to understand the most pressing IoT-related societal challenges. Given the vast extent of relevant technical literature, the difficulty was to concentrate research on the societal level. The research for this TA also addressed IoT-related issues specific to the defense sector in regard to each section of the TA.

The literature review highlighted the heterogeneity of definitions of the IoT and narrowed the initial research focus down on establishing a holistic, inclusive definition of the IoT:

> The IoT is a cyber-physical array of trans-sectoral pervasive network-ecosystems which is made up of the interconnection of multiple connected devices and the data they share via information and communication technologies. The ecosystem is understood in this TA as a „*network of interactions among organisms, and between organisms and their environment*" (ICANN) (in order to encompass the societal, systemic and technical aspects of the IoT). The IoT is considered to be a trans-sectoral and societal phenomenon, as it is present in almost all aspects of daily life and affects all sectors of society (e.g. home automation, the health and entertainment industries, aerospace industry, critical infrastructures, defense industry, etc.).
>
> In this regard, IoTs are defined as all the physical and virtual connected devices which sense, compute and interact with each other without regular human intervention. Such intervention is usually needed, though, when the "self-management capabilities of the (IoT ecosystem) are exhausted" (Avsystem, 2019).

This first step created the framework which allowed the multifaceted, multi-layered, and trans-societal nature of the IoT ecosystem and its security issues to be addressed in a second step. The analysis revealed that IoT-related technologies have accrued high business value because of the numerous benefits they deliver to society: higher connectivity, automation and control, increased revenue and cost savings as well as higher effectiveness in big data collection and analysis.

IoT business has become so valuable that it has given rise to a trend where security is traded off against costs, leading to the frenetic production of poorly secured IoT devices, regardless of the security, safety and lifecycle management aspects of the IoT ecosystem.

This lack of security considerations creates room for various misuses of the IoT. These are summarized and analyzed in this TA in the form of a threat taxonomy and an indicative timeline of prominent IoT-related security incidents and penetration testing in section 5.1.

This reflection on IoT-related incidents has shown that the IoT ecosystem is used both as a means and as a target for malicious acts. Furthermore, IoT ecosystems are likely to represent a major security gap due to the ease of hacking IoT devices, inadequate IoTs lifecycle management, and the significant number of poorly secured IoT devices already deployed across the fabric of societies, ranging from multimedia devices to critical infrastructures.

Even if regulating the IoT ecosystem at the national or international level will not solve the problem, because, as seen above, it is already too late, regulation may give society enough time to come up with a solution. Relevant stimuli for international organizations and governments highlight just how much is still left to be done: First, the most recent national cybersecurity strategies, apart from exceptions like Japan, indicate a poor level of awareness of IoT issues (Switzerland's 2018 cybersecurity strategy, for example, only refers to the IoT once). Second, no homogenous mandatory regulation of IoT-related security, safety, lifecycle management or data privacy has to date been established for industry or manufacturers.

Even though the above-mentioned IoT-related attacks (mostly Mirai) acted as an eye opener for civil society, international organizations and governments, this wake-up call came too late for two reasons: It happened *a posteriori* of the incidents and only after a critical mass of poorly secured IoTs had already been widely and deeply deployed in the fabric of society.

This large volume of IoTs has to be considered as critical because research has demonstrated that the existing number of IoTs is sufficient to create infections that "*will spread explosively over large areas in a kind of nuclear chain reaction*" (Ronen, 2018). Moreover, other studies have shown that 84% of a research pool of 3100 IoTs adopters had already experienced security breaches (Maddox, 2017). Finally, too many of the IoTs on the market are already dysfunctional and can no longer be replaced.

This brings us to an even broader issue: Our comprehensive analysis of IoT-related vulnerabilities, the reasons why these vulnerabilities still exist, the economics of the IoT, its regulation, and governmental decision-making and risk management related to the IoT ecosystem, persistently points towards one common, core vulnerability: the human factor. Indeed, lack of knowledge, poor cybersecurity hygiene, lax – in some cases even *laissez-faire* – market behavior, decision-making and regulation, as well as cost-benefit math at the expense of overall security and safety are all the result of human reasoning. The overall mindset regarding the security of the IoT ecosystem needs to change if security, safety and associated economic models are to be improved.

The IoT, as a global and trans-sectoral phenomenon, affects the defense sector the same way it affects any other social sphere. However, due to the critical nature of defense-sector structures, the consequences of poorly secured IoT systems are vastly more serious in this domain. The defense sector and the armed forces cannot afford the consequences of a *laissez-faire* trade-off between IoT costs and security on the market, if tanks like the Uran 9 are deployed in battlefields, for example.

Finally, complex societal systems are fragile and have come to rely increasingly on IoT ecosystems in industrialized countries, rendering them even more vulnerable for the following reasons: There is currently no guarantee that IoTs are safe and secure; it is difficult to control their lifecycle or to shut them down without shutting down important societal processes; increased reliance on IoTs increases dependence on such systems; and finally IoTs have become essential for the proper functioning of entire societies. Going forward, if secure and safe IoT ecosystems are to become economically viable, it is essential that the shortcomings of the past with regard to poor IoT security would be addressed and the vicious cycle of prioritizing economic benefits over security and safety be broken. However, if the safety and the security of the IoT cannot be guaranteed, alternative solutions would be required.

9 Annex

List of states' cybersecurity and / or cyberdefense strategies used in the word search for section 3.4

°	Country	Strategy title	Year of publication	# "IoT	# "Internet of Things"	# "internet of things"	Total # "IoT" + "Internet of things" + "internet of things"
1.	Afghanistan	National Cyber Security Strategy of Afghanistan	2014	-	-		-
2.	Australia	Cyber Security Strategy	2009				
3.	Australia	Cybersecurity Strategy	2016		4		4
4.	Austria	National ICT Security Strategy Austria	2012				
5.	Austria	Austrian Cyber Security Strategy	2013		1		1
6.	Bangladesh	National Cyber Security Strategy	2014				
7.	Belgium	Cyber Security Strategy. Securing Cyberspace	2012				
8.	Belgium	Defense Cyber Security Strategy	2014				
9.	Canada	Canada's Cyber Security Strategy	2010				
10.	Canada	Action Plan 2010 -2015 for Canada's Cyber Security Strategy	2013	-	-		-
11.	Canada	National Cyber Security Strategy	2018	2	-		2
12.	Chile	National Cybersecurity Policy	2017				
13.	China	National Cyberspace Security Strategy	2016				
14.	Colombia	National Cybersecurity and Cyberdefense Policy	2011				
15.	Croatia	The National Cyber Security Strategy of the Republic of Croatia	2015	1	1		2
16.	Cyprus	The National Cyber Security Strategy of the Republic of Cyprus	2012				
17.	Czech Republic	National Cyber Security Strategy of the Czech Republic from the period from 2015 to 2020	2015	2	-		2
18.	Denmark	Danish Cyber and Information Security Strategy	2015				
19.	Denmark	A stronger and more secure digital Denmark	2016	1	1		2
20.	Egypt	National ICT Strategy 2012-2017	2012				
21.	Estonia	Cyber Security Strategy 2014-2017	2014				
22.	Finland	Security Strategy for Society	2010				
23.	Finland	Finland's Cyber Security Strategy Background Dossier	2013				
24.	Finland	Finland's Cyber security Strategy	2013				
25.	France	Information Systems Defense and Security - France's Strategy	2011				
26.	France	French National Digital Security Strategy	2015				
27.	Georgia	Cyber Security Strategy of Georgia 2012-2015	2012				

°	Country	Strategy title	Year of publication	# "IoT	# "Internet of Things"	# "internet of things"	Total # "IoT" + "Internet of things" + "internet of things"
28.	Germany	Cyber Security Strategy for Germany	2011				
29.	Ghana	Ghana National Cyber Security Policy and Strategy	2014				
30.	Greece	National Cyber Security Strategy	2017				
31.	Hungary	National Cyber Security Strategy of Hungary	2013				
32.	Iceland	Icelandic National Cyber Security Strategy 2015–2026	2015				
33.	India	National Cyber Security Policy 2013	2013				
34.	Ireland	National Cyber Security strategy 2015-2017	2015				
35.	Israel	Advancing National Cyberspace Capabilities	2011				
36.	Italy	National Strategic Framework for Cyberspace Security	2013	2	1	-	3
37.	Jamaica	National Cyber Security Strategy	2015	3	2		5
38.	Japan	International Strategy on Cybersecurity Cooperation	2013	-	-	-	
39.	Japan	Cybersecurity Strategy – Toward a World-Leading, Resilient and Vigorous Cyberspace	2013	-	1		1
40.	Japan	Cybersecurity Strategy	2015	54	2	-	56
41.	Japan	Cybersecurity Strategy	2018	37	1		38
42.	Jordan	National Information Assurance and Cyber Security Strategy	2012				
43.	Kenya	Cybersecurity Strategy	2014				
44.	Korea	Cyber Security Masterplan					
45.	Latvia	Cyber Security Strategy of Latvia 2014-2018	2014				
46.	Kuwait	National Cyber Security Strategy for the State of Kuwait	2017				
47.	Kyrgyzstan	The Development Program of the Kyrgyz republic for the period 2018-2022	2018				
48.	Liechtenstein	Priorities of Liechtenstein Foreign Policy	2012				
49.	Lithuania	Programme for the development of electronic information security (cyber-security) for 2011-2019	2011				
50.	Luxembourg	National Cybersecurity Strategy II	2015				
51.	Luxembourg	National Cybersecurity Strategy III	2018	-	-	2	2
52.	Macedonia	Republic of Macedonia National Cyber Strategy 2018-2022	2018	3	1		4
53.	Malawi	National ICT Policy	2013				

°	Country	Strategy title	Year of publication	# "IoT	# "Internet of Things"	# "internet of things"	Total # "IoT" + "Internet of things" + "internet of things"
54.	Malaysia	National Cyber Security	2006				
55.	Malta	Malta Cyber Security Strategy 2016	2016				
56.	Mauritius	National Cyber Security Strategy 2014-2019	2014				
57.	Mexico	National Cybersecurity Strategy	2017				
58.	Micronesia	The Federated States of Micronesia National ICT and Telecommunications Policy	2012				
59.	Moldova	National Strategy for information society development "Digital Moldova 2020"	2013				
60.	Montenegro	National Cyber Security Strategy of Montenegro 2018-2021	2017	4	5	-	9
61.	Morocco	National Strategy for Information Society and Digital Economy ("Digital Morocco 2013")	2013				
62.	Netherlands	The Defense Cyber Strategy	2012				
63.	Netherlands	National Cyber Security Strategy 2	2013				
64.	Netherlands	National Cyber Security Strategy 3	2018				
65.	New Zealand	New Zealand's Cyber Security Strategy	2011				
66.	New Zealand	New Zealand's Cyber Security Strategy	2015				
67.	Nigeria	National cybersecurity Policy	2014				
68.	Norway	Cyber Security Strategy for Norway	2012				
69.	Philippines	Philippine National Cyber Security Plan 2005	2005				
70.	Poland	Governmental Program for Protection of Cyberspace for the years 2011-2016	2013				
71.	Portugal	National Cyber Security Strategy	2015				
72.	Qatar	Qatar National Cyber Security Strategy	2014				
73.	Republic of Korea	National Cyber Security Masterplan	2011				
74.	Russia	Information Security Doctrine of the Russian Federation	2000				
75.	Russia	Basic Principles for State Policy of the Russian Federation in the Field of International Information Security	2013				
76.	Rwanda	Rwanda National ICT Strategy and Plan	2011				
77.	Rwanda	Rwanda ICT Strategic and Action Plan	2015				
78.	Saint Vincent and the Grenadines	National Information and Communication Technology Strategy and Action Plan	2010				

	Country	Strategy title	Year of publication	# "IoT	# "Internet of Things"	# "internet of things"	Total # "IoT" + "Internet of things" + "internet of things"
79.	Samoa	Samoa National Cybersecurity Strategy 2016-2021	2016				
80.	Saudi Arabia	National Information Security Strategy in Saudi Arabia	2013				
81.	Senegal	Senegalese National Strategy (SNC2022)	2017	-	3		3
82.	Singapore	National Cyber Security Masterplan 2018	2013				
83.	Singapore	Singapore's Cybersecurity Strategy	2016	-	1		1
84.	Slovakia	National Strategy for Information Security in the Slovak Republic	2008				
85.	Slovakia	Cyber Security Concept of the Slovak Republic for 2015-2020	2015				
86.	Slovenia	Cyber Security Strategy	2016				
87.	South Africa	National Cybersecurity Policy Framework for South Africa	2015				
88.	Spain	National Cyber Security, a Commitment for Everybody	2012				
89.	Spain	National Cyber Security Strategy	2013				
90.	Sri Lanka	Information and Cyber Security Strategy of Sri Lanka 2019 -2023	2018				
91.	Switzerland	National strategy for Switzerland's protection against cyber risks	2012				
92.	Switzerland	National strategy for the protection of Switzerland against cyber risks (NCS) 2018-2022	2018	-	-	1	1
93.	Taiwan	National Cyber Security Program of Taiwan (2017 to 2020)	2017	1	26		27
94.	Tanzania	National Information and Communications Technologies Policy	2003				
95.	Trinidad and Tobago	National Cyber Security Strategy	2012				
96.	Turkey	National Cyber Security Strategy and 2013-2014 Action Plan	2013				
97.	Turkey	2016-2019 National Cyber Security Strategy	2016				
98.	Uganda	National Information Security Strategy	2011				
99.	Uganda	National Information Security Policy	2014				
100.	United Arab Emirates	Dubai Cyber Security Strategy	2017	3	-	2	5
101.	United Kingdom	Cyber Security Strategy of the United Kingdom	2011				
102.	United Kingdom	National Cyber Security Strategy 2016-2021	2016	2	7		9
103.	United States of America	The National Strategy to Secure Cyberspace	2003				
104.	United States of America	Cyberspace Policy Review	2009				

°	Country	Strategy title	Year of publication	# "IoT	# "Internet of Things"	# "internet of things"	Total # "IoT" + "Internet of things" + "internet of things"
105.	United States of America	International Strategy for Cyberspace - Prosperity, Security, and Openness in a Networked World	2011				
106.	United States of America	Department of Defense Strategy for Operating in Cyberspace	2011				
107.	United States of America	The DOD Cyber Strategy	2015				
108.	Vanuatu	National Cybersecurity Policy	2013				
109.	Zambia	Zambia Information and Communication Technology Policy	2006				
110.	Zimbabwe	National Policy for ICT 2016-2020	2016				
TOTAL				11	56	5	176

10 Glossary

Attribution problem: Difficulty to determine with certainty the perpetrator of a cyberattack. Attackers are more difficult to identify because of their ability to cover tracks, perform spoof cyberattacks, or falsely flag other actors as perpetrators (Hay Newman, 2016).

Botnet or bot: Network of infected computers which can be accessed remotely and controlled centrally in order to launch coordinated attacks (Ghernaouti-Hélie, 2013, p. 427).

Bricking: Damaging an electronic device to the point that it is “as useful as a brick” (PCmag, 2018).

Distributed Denial of Service (DDoS): The act of overwhelming a system with a large number of packets through the simultaneous use of infected computers (Ghernaouti-Hélie, 2013, p. 431).

Exploit: An attack on a computer operating system using a vulnerability of the system or software (Rouse, 2017).

Hack: Act of entering a system without authorization (Ghernaouti-Hélie, 2013, p. 433).

Malware: Malicious software that can take the form of a virus, a worm or a Trojan horse (Collins and McCombie, 2012, p. 81).

Peer to Peer (P2P): Computer systems connected in a network that enables the direct sharing of files between them without the need for a central server (TechTerms, 2016).

Siemens Simatic WinCC/Step-7 software: Industrial software serving as human-machine interface (Lindsay, 2013, p. 380).

Social engineering: A non-technical strategy cyber attackers use that relies heavily on human interaction and often involves tricking people into breaking standard security practices (Lord, 2015).

Spoofing: Act of usurping IP addresses in order to commit malicious acts such as breaching a network (Ghernaouti-Hélie, 2013, p. 440).

Supervisory Control And Data Acquisition (SCADA): Computer programs used to control industrial processes (Langner, 2013, p. 9).

11 Abbreviations

4 G	4th Generation mobile communication
5 G	5th Generation mobile communication
ABS	Anti-lock Braking System
APT	Advanced Persistent Threats
CIoTs	Customer Internet of Things
CSO	Information Systems Collaborative Support Office
CT	Customer Technology
DCMS	Department for Digital, Culture, Media and Sport
DDoS	Distributed Denial of Service attack
EEE	European Economic Area
ENISA	European Union Agency for Network and Information Security
EU	European Union
FBI	Federal Bureau of Investigation
FoM	Freedom of Movement
FTC	Federal Trade Commission
GBPS	Gigabytes per Second
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HMI	Human Machine Interface
ICS	Critical Control Systems
ICTs	Information and Communication Technologies
IoT	Internet of Things
IoTs	Internet of Things’ connected objects
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunication Union
M2M	Machine to Machine
NATO	North Atlantic Treaty Organization
NATO STANAG	NATO Standardization Agreement
NICT	Japanese National Institute of Information and Communications Technology
OT	Operational Technology
P2P	Peer-to-Peer
PLA	Chinese People's Liberation Army
POLIMI	Italian Technical University Politecnico di Milano
RFID	Radio Frequency Identification
SASE	Safe and Secure Environment
SCADA	Supervisory Control and Data Acquisition
TBPS	Terabyte per Second

UK	United Kingdom
UN	United Nations
UN/CEFACT	UN Centre for Trade Facilitation and E-business
USA	United States of America

12 Bibliography

AFP, 2019. Japan to survey 200 million devices in cybersecurity push ahead of Tokyo 2020 Olympics. Jpn. Times Online.

Ajay Kumar Maurya, Ahmad, J., 2018. IoT Based Comprehensive Monitoring Of Network And Related Infrastructure. Int. J. Adv. Res. Comput. Sci. 9.

Amyx, S., 2014. Why the Internet of Things Will Disrupt Everything. Wired.

Arashi, R., Midgley, J., Fly Perdersen, L., Pelczar, J., Hillock Wellington, A., Rickert, G., Jones, S., Auckland, L., 2017. Defense Policy and the Internet of Things: Disrupting Global Cyber Defenses.

Ashford, W., 2018. IoT firms sign up to UK security code of practice [WWW Document]. ComputerWeekly.com. URL https://www.computerweekly.com/news/252450588/IoT-firms-sign-up-to-UK-security-code-of-practice (accessed 27.03.2019).

Ashton, K., 2019. That “Internet of Things” Thing. RFID J. URL https://www.rfidjournal.com/articles/view?4986

Associated Press, 2017. Three men plead guilty in case of cyber-attack that paralyzed internet in 2016 [WWW Document]. The Guardian. URL https://www.theguardian.com/technology/2017/dec/13/mirai-botnet-cyber-attack-2016-men-plead-guilty (accessed 29.08.2018).

Audio Software Engineering and Siri Speech Team, 2018. Optimizing Siri on HomePod in Far-Field Settings [WWW Document]. Apple Mach. Learn. J. URL https://machinelearning.apple.com/2018/12/03/optimizing-siri-on-homepod-in-far-field-settings.html (accessed 02.08.2019).

Avsystem, 2019. What is Internet of Things (IoT)? – Everything you Need to Know [WWW Document]. Avsystem.com. URL https://www.avsystem.com/blog/what-is-internet-of-things-explanation/ (accessed 02.08.2019).

Baezner, M., Robin, P., 2018. Trend Analysis: Cyber Sovereignty and Data Sovereignty. Cyber Defense Project 40.

Baezner, M., Robin, P., 2017. Hotspot Analysis: Stuxnet.

Barrera, J., 2015. Hacker told F.B.I. he made plane fly sideways after cracking entertainment system [WWW Document]. aptnews.ca. URL https://aptnnews.ca/2015/05/15/hacker-told-f-b-made-plane-fly-sideways-cracking-entertainment-system/ (accessed 06.08.2019).

Bode, K., 2018. The Internet of Things Needs Food Safety-Style Ratings for Privacy and Security [WWW Document]. Motherboard. URL https://motherboard.vice.com/en_us/article/a3qyek/the-internet-of-things-needs-food-safety-style-

ratings-for-privacy-and-security (accessed 28.08.2018).
Bonderud, D., 2018. Leaked Mirai Malware Boosts IoT Insecurity Threat Level. Secur. Intell. URL https://securityintelligence.com/news/leaked-mirai-malware-boosts-iot-insecurity-threat-level/ (accessed 04.04.2019).
Bur, J., 2017. IoT is changing the meaning of ‘critical infrastructure’ [WWW Document]. Fed. Times. URL https://www.federaltimes.com/smr/cybercon/2017/11/29/iot-is-changing-the-meaning-of-critical-infrastructure/ (accessed 04.09.2018).
Carhart, L., 2018. Do renters have the right to reject smart home technology? | Thinklab [WWW Document]. URL https://thinklab.com/content/4077826 (accessed 16.04.2019).
Chan, B., 2017. Future-proofing your IoT Infrastructure. Strategy Things. URL https://strategyofthings.io/future-proofing-iot (accessed 26.03.2019).
Chow, E.K., 2018. Russia Just Showed Off Its New Robot Tank — And Confirmed It Was On The Ground In Syria [WWW Document]. Task Purp. URL https://taskandpurpose.com/russia-uran-9-robot-tank-syria (accessed 04.04.2019).
Clausewitz, C. von, 2008. On War. Princeton University Press.
Colin, N., Verdier, H., 2012. L’économie de la multitude. ParisTech Rev.
Collins, S., McCombie, S., 2012. Stuxnet: the emergence of a new cyber weapon and its implications. J. Polic. Intell. Count. Terror. 7, 80–91. https://doi.org/10.1080/18335330.2012.653198
Dabbagh, M., Rayes, A., 2017. Internet of Things Security and Privacy, in: Internet of Things From Hype to Reality. Springer International Publishing, Cham, pp. 195–223. https://doi.org/10.1007/978-3-319-44860-2_8
Darwish, A., Hassanien, A.E., Elhoseny, M., Sangaiah, A.K., Muhammad, K., 2017. The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems. J. Ambient Intell. Humaniz. Comput. https://doi.org/10.1007/s12652-017-0659-1
Daws, R., 2016. Another IoT-based DDoS attack leaves Finnish properties without heating [WWW Document]. IoT Tech News. URL https://www.iottechnews.com/news/2016/nov/08/another-iot-based-ddos-attack-leaves-finnish-properties-without-heating/ (accessed 04.04.2019).
DCMS, 2019. Secure by Design [WWW Document]. GOV.UK. URL https://www.gov.uk/government/collections/secure-by-design (accessed 27.03.2019).
DefenseWorld.net, 2018. Chinese Combat Soldiers Get New Smart Watches [WWW Document]. DefenseWorld.net. URL http://www.defenseworld.net/news/23861/Chinese_Combat_Soldiers_Get_New_Smart_Watches#.XI-UE7hCfmE (accessed 18.03.2019).
Dewar, R.S., 2017. Trend Analysis: Cyberweapons: Capability, Intent and Context in Cyberdefense. Cyber Defense Project 24.
Duffy, J., 2014. 8 Internet things that are not IoT [WWW Document]. Netw. World. URL https://www.networkworld.com/article/2378581/internet-of-things/8-internet-things-that-are-not-iot.html (accessed 14.02.2019).
Economics Online, 2018. Negative externalities, Third-party costs [WWW Document]. Econ. Onlinecouk. URL https://www.economicsonline.co.uk/Market_failures/Externalities.html (accessed 26.03.2019).
ENISA, 2017. Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures.
EU Council, 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L.
European Commission, 2017. Proposal for a Regulation: Cybersecurity Package. COM(2017)477.
Fraga-Lamas, P., Fernández-Caramés, T., Suárez-Albela, M., Castedo, L., González-López, M., 2016. A Review on Internet of Things for Defense and Public Safety. Sensors 16, 1644. https://doi.org/10.3390/s16101644
Franceschi-Bicchierai, L., 2017a. The Hackers Behind Some of the Biggest DDoS Attacks in History Plead Guilty [WWW Document]. Motherboard. URL https://motherboard.vice.com/en_us/article/d3xykq/hackers-behind-mirai-ddos-botnet-plea-guilty (accessed 08.08.2018).
Franceschi-Bicchierai, L., 2017b. How This Internet of Things Stuffed Animal Can Be Remotely Turned Into a Spy Device. Motherboard. URL https://motherboard.vice.com/en_us/article/qkm48b/how-this-internet-of-things-teddy-bear-can-be-remotely-turned-into-a-spy-device (accessed 04.04.2019).
Franceschi-Bicchierai, L., 2015a. When the Internet of Things Starts to Feel Like the Internet of Shit. Motherboard. URL https://motherboard.vice.com/en_us/article/pgkdm7/when-the-internet-of-things-starts-to-feel-like-the-internet-of-shit (accessed 22.03.2019).
Franceschi-Bicchierai, L., 2015b. VTech Hacker Explains Why He Hacked the Toy Company. Motherboard. URL https://motherboard.vice.com/en_us/article/xygg9

w/vtech-hacker-explains-why-he-hacked-the-toy-company (accessed 04.04.2019).
FTC, 2015a. FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks [WWW Document]. Fed. Trade Comm. URL https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices (accessed 27.03.2019).
FTC, 2015b. Internet of Things, Privacy & Security in a Connected World. USA Federal Trade Commission.
Fu, Kevin, Kohno, T., Lopresti, D., Mynatt, E., Nahrstedt, K., Patel, S., Richardson, D., Zorn, B., 2017. Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things.
Ghernaouti-Hélie, S., 2013. Cyberpower: crime, conflict and security in cyberspace, 1. ed. ed, Forensic sciences. EPFL Press, Lausanne.
GICHD, 2013. Digger D - 3 [WWW Document]. Geneva Int. Cent. Humanit. Demining. URL https://www.gichd.org/resources/equipment-catalogue/mechanical/equipment/digger-d-3/ (accessed 04.04.2019).
Gloria, D., 2016. STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT).
Grebler, L., 2017. Why Do IoT Devices Die? IoT All. URL https://medium.com/iotforall/why-do-iot-devices-die-e4df0c7a075d (accessed 22.03.2019).
Hausenbla, M., 2014. Smart Phones and the Internet of Things |. MapR. URL https://mapr.com/blog/smart-phones-and-internet-things/ (accessed 07.03.2019).
Hay Newman, L., 2016. Hacker Lexicon: What is the Attribution Problem? [WWW Document]. WIRED. URL https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/ (accessed 12.01.2019).
ICANN, 15:57:03 UTC. ICANN and the Internet Ecosystem.
Inside Privacy, 2018. IoT Update: The UK publishes a final version of its Code of Practice for Consumer IoT Security [WWW Document]. Priv. URL https://www.insideprivacy.com/internet-of-things/iot-update-the-uk-publishes-a-final-version-of-its-code-of-practice-for-consumer-iot-security/ (accessed 27.03.2019).
IoT Ecosystem, 2016. Defining the IoT Ecosystem for Enterprises [WWW Document]. IoT Innov. URL https://internet-of-things-innovation.com/insights/the-blog/defining-iot-ecosystem-enterprises/ (accessed 14.03.2019).
IoT Security Watch, 2018. GhostDNS: the botnet made up of 100,000 routers is attacking Brazil [WWW Document]. IoT Secur. Watch. URL https://iotsecuritywatch.com/en/2018/10/31/botnet-ghostdns-the-botnet-made-up-of-100000-routers-is-attacking-brazil/ (accessed 04.04.2019).
Ireland, E., 2001. Puerto Rico smart meters believed to have been hacked – and such hacks likely to spread [WWW Document]. Smart Energy Int. URL https://www.smart-energy.com/regional-news/north-america/puerto-rico-smart-meters-believed-to-have-been-hacked-and-such-hacks-likely-to-spread/ (accessed 04.04.2019).
ISO, 2019. ISO/IEC 21823-1:2019 (en), Internet of things (IoT) -- Interoperability for internet of things systems [WWW Document]. ISO. URL http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/18/71885.html (accessed 17.04.2019).
ISO, 2018. ISO/IEC 30141:2018(en), Internet of Things (loT) — Reference Architecture [WWW Document]. iso.org. URL https://www.iso.org/obp/ui/#iso:std:iso-iec:30141:ed-1:v1:en (accessed 26.03.2019).
ITU, 2019. National Strategies [WWW Document]. itu.int. URL https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx (accessed 29.03.2019).
ITU, 2005. The Internet of Things.
ITU-T, 2012. Recommendation ITU-T Y.4000/Y.2060: Overview of the Internet of things.
ITU-T, n.d. ITU-T: Global Standards for the Internet of Things [WWW Document]. itu.int. URL https://www.itu.int/en/ITU-T/techwatch/Pages/internetofthings.aspx (accessed 26.03.2019).
Jia, X., Feng, Q., Fan, T., Lei, Q., 2012. RFID technology and its applications in Internet of Things (IoT), in: 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet). Presented at the 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), pp. 1282–1285. https://doi.org/10.1109/CECNet.2012.6201508
Jungo, C., 2015. Integrity and trust in the Internet of Things 13.
Kan, M., 2016. Upgraded Mirai botnet disrupts Deutsche Telekom by infecting routers [WWW Document]. Computerworld. URL https://www.computerworld.com/article/3145372/upgraded-mirai-botnet-disrupts-deutsche-telekom-by-infecting-routers.html (accessed 04.04.2019).
Kaspersky Lab, 2017. 300,000 obeying devices: Hajime is conquering the Internet of Things world | Kaspersky Lab [WWW Document]. Kaspersky.com. URL https://www.kaspersky.com/about/press-releases/2017_300000-obeying-devices-hajime-is-conquering-the-internet-of-things-world (accessed 04.04.2019).
Keller, J., 2019. Russia's robot tank sucks, but its military is adopting it anyway [WWW Document]. Task Purp. URL https://taskandpurpose.com/russia-army-adopting-uran-9-robot-tank (accessed 04.04.2019).

Kersting, K., Meyer, U., 2018. From Big Data to Big Artificial Intelligence? KI - Künstl. Intell. 32, 3–8. https://doi.org/10.1007/s13218-017-0523-7
Khaddar, M.A.E., Boulmalf, M., 2017. Smartphone: The Ultimate IoT and IoE Device. Smartphones Appl. Res. Perspect. https://doi.org/10.5772/intechopen.69734
Kilbride, J., Xiao, B., 2018. World's most popular drones wide open to spying after Chinese manufacturer's flaw revealed [WWW Document]. ABC News. URL https://www.abc.net.au/news/2018-11-14/dji-drones-were-exposed-to-security-flaw/10491150 (accessed 04.04.2019).
Kleinhans, J.-P., 2019. 5G vs. National Security.
Kleinhans, J.-P., 2018. Standardisierung & Zertifizierung in der IT-Sicherheit.
Kleinhans, J.-P., 2017. Internet of Insecure Things.
Kranz, M., 2018. IoT For Economic And Social Good: How The Internet Of Things Makes Our World Better [WWW Document]. Forbes. URL https://www.forbes.com/sites/forbestechcouncil/2018/06/14/iot-for-economic-and-social-good-how-the-internet-of-things-makes-our-world-better/ (accessed 15.03.2019).
Langner, R., 2013. To kill a centrifuge: a technical analysis of what Stuxnet's creators tried to achieve.
Lewis, J.A., 2016. Managing Risk for the Internet of Things [WWW Document]. Cent. Strateg. Int. Stud. URL https://www.csis.org/blogs/strategic-technologies-blog/managing-risk-internet-things (accessed 21.08.2018).
Lindsay, J.R., 2013. Stuxnet and the Limits of Cyber Warfare. Secur. Stud. 22, 365–404. https://doi.org/10.1080/09636412.2013.816122
Lord, N., 2015. What is Social Engineering? Defining and Avoiding Common Social Engineering Threats [WWW Document]. Digit. Guard. URL https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats (accessed 13.10.2017).
Maddox, T., 2017. Enterprise IoT adoption to hit critical mass by 2019, but security remains a top concern [WWW Document]. TechRepublic. URL https://www.techrepublic.com/article/enterprise-iot-adoption-to-hit-critical-mass-by-2019-but-security-remains-a-top-concern/ (accessed 06.06.2019).
Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., Aharon, D., 2015. The Internet Of Things: Mapping The Value Beyond The Hype.
Michel, R., 2017. The Operations Technology (OT) vs. Information Technology (IT) Debate Turns to Better Security [WWW Document]. Supplycahin247.com. URL https://www.supplychain247.com/article/the_operations_technology_ot_vs._information_technology_it_debate_turns_to/Information_Management (accessed 18.03.2019).
Military-Today, n.d. Keiler Mine Clearing Vehicle [WWW Document]. Mil.-Todaycom. URL http://www.military-today.com/engineering/keiler.htm (accessed 04.04.2019).
Novak, M., 2018. Fitness App's "Anonymized" Data Dump Accidentally Reveals Military Bases Around the World [WWW Document]. Gizmodo. URL https://gizmodo.com/fitness-apps-anonymized-data-dump-accidentally-reveals-1822506098 (accessed 04.04.2019).
Ochs, T., 2017. Internet of Things The Power of the IoT Platform, in: Ramachandran, M., Méndez Muñoz, V., Kantere, V., Wills, G., Walters, R., Chang, V. (Eds.), IoTBDS 2017: Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security: Porto, Portugal, April 24-26, 2017. SCITEPRESS - Science and Technology Publications, Lda, Setúbal, Portugal, pp. 284–294.
Openshaw, E., Haegel, J., Wooll, M., Wigginton, C., Seely Brown, J., Banerjee, P., 2014. The Internet of Things Ecosystem.
Paganini, P., 2016a. Flaws in BMW ConnectedDrive Infotainment System allow remote hack [WWW Document]. Secur. Aff. URL https://securityaffairs.co/wordpress/49149/hacking/bmw-connecteddrive-hacking.html (accessed 04.04.2019).
Paganini, P., 2016b. PanelShock 0-day Vulnerability Puts Thousands of Schneider Electric HMI Panels, Industrial Control Systems and Critical Infrastructure at Risk [WWW Document]. Secur. Aff. URL https://securityaffairs.co/wordpress/52945/hacking/schneider-electric-0-day-flaws.html (accessed 04.04.2019).
Paratus People Limited, 2018. A Timeline of IoT Hacks and Vulnerabilities [WWW Document]. ParatusPeople.com. URL https://www.paratuspeople.com/news/a-timeline-of-iot-hacks-and-vulnerabilities/38576/ (accessed 22.03.2019).
PCmag, 2018. Definition of: brick [WWW Document]. PCmag. URL https://www.pcmag.com/encyclopedia/term/58448/brick (accessed 18.06.2018).
Piedad, F.N., n.d. IoT apps trend: 3 essential ingredients for success [WWW Document]. TechBeacon. URL https://techbeacon.com/security/iot-apps-trend-3-essential-ingredients-success (accessed 14.03.2019).
Rachid, F., 2018. Hacker History: The Time Charlie and Chris Hacked a Jeep Cherokee [WWW Document]. Decipher. URL https://duo.com/decipher/hacker-history-time-charlie-chris-hacked-jeep-cherokee (accessed 04.04.2019).

Radichel, T., 2014. Case Study: Critical Controls that Could Have Prevented Target Breach 32.

Rifkin, J., 2012. La troisième révolution industrielle. LES LIENS QUI LIBERENT EDITIONS, Paris.

Ronen, E., 2018. IoT Goes Nuclear: Creating a ZigBee Chain Reaction [WWW Document]. Eyal Ronen. URL http://www.eyalro.net/project/iotworm/ (accessed 06.08.2019).

Rouse, M., 2017. Computer exploit [WWW Document]. TechTarget. URL http://searchsecurity.techtarget.com/definition/exploit (accessed 20.02.2019).

Ruche, S., 2019. Jeremy Rifkin: «La Suisse est le modèle idéal pour la prochaine révolution industrielle ».

Sattler, J., 2019. IoT Threat Landscape, Old Hacks new Devices. F-Secure.

Security Today, 2017. FDA Issues Recall on Pacemakers Due to Security Vulnerabilities - [WWW Document]. Secur. Today. URL https://securitytoday.com/articles/2017/08/31/pacemaker-recall.aspx (accessed 04.04.2019).

Segal, L., 2016. Mirai: The IoT Bot that Took Down Krebs and Launched a Tbps Attack on OVH [WWW Document]. F5 Labs. URL https://www.f5.com/labs/articles/threat-intelligence/mirai-the-iot-bot-that-took-down-krebs-and-launched-a-tbps-attack-on-ovh-22422.html (accessed 16.04.2019).

SGDSN, 2018. Revue Stratégique de Cyberdéfense.

Shah, S., 2017. BrickerBot creator Janit0r “retires” after bricking over 10 million IoT devices. Internet Bus. URL https://internetofbusiness.com/brickerbot-janit0r-retires/ (accessed 04.04.2019).

Sicari, S., Rizzardi, A., Cappiello, C., Miorandi, D., Coen-Porisini, A., 2018. Toward Data Governance in the Internet of Things, in: Yager, R.R., Pascual Espada, J. (Eds.), New Advances in the Internet of Things, Studies in Computational Intelligence. Springer International Publishing, Cham, pp. 59–74. https://doi.org/10.1007/978-3-319-58190-3_4

Slowey, L., 2017. IoT benefits, challenges, and opportunities: CES 2017, in: IBM Internet of Things Blog. Presented at the IoT benefits, challenges, and opportunities: CES 2017, IBM, Las Vegas.

Son, H., Kim, S., 2012. Defense–in–Depth Strategy for Smart Service Sever Cyber Security, in: Kim, T., Ko, D., Vasilakos, T., Stoica, A., Abawajy, J. (Eds.), Computer Applications for Communication, Networking, and Digital Contents, Communications in Computer and Information Science. Springer Berlin Heidelberg, pp. 181–188.

State of California, 2018. Information privacy: connected devices., State Bill.

Stefanuk, A., 2017. Building Mobile Apps for IoT Projects : Statistics and Tendencies. TechBullion. URL https://www.techbullion.com/building-mobile-apps-for-iot-projects-statistics-and-tendencies/ (accessed 14.03.2019).

STO, 2019. STO-Activities - All Items [WWW Document]. sto.nato.int. URL https://www.sto.nato.int/Lists/test1/AllItems.aspx (accessed 30.03.2019).

Stone, J., 2019. Think of satellites as big, vulnerable IoT devices, researcher says [WWW Document]. CyberScoop. URL https://www.cyberscoop.com/satellites-cybersecurity-bill-malik-rsa/ (accessed 11.03.2019).

Swedberg, C., 2019. NATO Samples New GPS-Based Tags, Expands Active RFID Use - 2019-02-06 - Page 1 - RFID Journal [WWW Document]. RFIDjournal.com. URL https://www.rfidjournal.com/articles/view?18253 (accessed 26.03.2019).

Szoldra, P., 2016. Here’s how the “Internet of Things” is being used for major cyberattacks on corporations [WWW Document]. Bus. Insid. URL http://www.businessinsider.fr/us/internet-of-things-corporate-cyberattacks-2016-10 (accessed 05.09.2018).

Tapestry Solutions, 2017. How the IoT is Transforming Military Logistics; A Look at the Past & How ESI Can Help Today. Tapestry Solut. URL https://www.tapestrysolutions.com/2017/12/19/esi-and-the-iot-in-the-military-part-i-problems-from-the-past-and-how-the-internet-of-things-is-transforming-dod-supply-chain-management/ (accessed 18.03.2019).

TechTerms, 2016. P2P [WWW Document]. TechTerms. URL http://techterms.com/definition/p2p (accessed 08.12.2016).

Toffler, A., Toffler, H., Gibson, R., 2011. Rethinking the Future: Rethinking Business Principles, Competition, Control and Complexity, Leadership, Markets and the World. Hachette UK.

Tonin, M., 2017a. The Internet of Things: Promises And Perils Of Disruptive Technology (No. 175 STCTTS 17 E bis). NATO Parliamentary Assembly.

Tonin, M., 2017b. The Internet of Things: promises and perils of a disruptive technology (STC No. 175 STCTTS 17 E bis). NATO Parliamentary Assembly.

Tortonesi, M., Morelli, A., Govoni, M., Michaelis, J., Suri, N., Stefanelli, C., Russell, S., 2016. Leveraging Internet of Things within the military network environment — Challenges and solutions, in: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT). Presented at the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), IEEE, Reston, VA, USA, pp. 111–116. https://doi.org/10.1109/WF-IoT.2016.7845503

Trend Micro, 2017. Rogue Robots: Testing the Limits of an Industrial Robot’s Security [WWW Document]. URL https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/rogue-robots-testing-industrial-robot-security (accessed 04.04.2019).

Untersinger, M., 2017. Comment le virus Mirai a pu bloquer le Web américain pendant plusieurs heures [WWW Document]. Le Monde. URL https://www.lemonde.fr/pixels/article/2017/08/22/le-logiciel-mirai-responsable-de-plus-de-15-000-attaques_5175162_4408996.html (accessed 29.08.2018).

Vaas, L., 2015. Baby monitor hijacked; change default password urges Foscam. Naked Secur. URL https://nakedsecurity.sophos.com/2015/02/02/baby-monitor-hijacked-change-default-password-urges-foscam/ (accessed 04.04.2019).

Williams, R., 2015. Hackers manipulate self-aiming rifle into shooting different targets.

Williamson, G., 2015. OT, ICS, SCADA – What's the difference? [WWW Document]. KuppingerCole. URL https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference (accessed 06.08.2019).

Zheng, D.E., Carter, W.A., CSIS Strategic Technologies Program, Center for Strategic and International Studies (Washington, D.C.., 2015. Leveraging the internet of things for a more efficient and effective military.

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.