STC

175 STCTTS 17 E bis
Original: English

NATO Parliamentary Assembly

SCIENCE AND TECHNOLOGY COMMITTEE

THE INTERNET OF THINGS: PROMISES AND PERILS OF A DISRUPTIVE TECHNOLOGY

REPORT

Matej TONIN (Slovenia)
Rapporteur
Sub-Committee on Technology Trends and Security

TABLE OF CONTENTS

I. INTRODUCTION

1. The Internet of Things (IoT) has rightly been a technology buzzword for several years: it has the potential to disrupt modern life as we know it. Today, more connected objects exist on the planet than people. In 2016, while the world's human population stood at 7.4 billion people, the number of connected devices reached about 16.28 billion (Cisco, 2016). By 2020, between 30 and 60 billion devices will be connected worldwide (Vermesan et al., 2015; Howard, 2016). The IoT's economic impact already totals about USD 2 trillion annually, and by 2025, the global IoT market could account for USD 4 to 12.8 trillion per year (Fischer, 2015; Al-Fuhaqa et al., 2015).

2. The rapid growth of IoT technology is driven by four key developments (Zheng & Carter, 2015). First, sensors, controllers and transmitters are becoming more powerful, cheaper and smaller. Second, internet penetration, bandwidth and the availability of wireless connectivity is increasing rapidly. Third, data storage and processing capacity are becoming bigger and better, making it easier and more affordable to store and organise data. Finally, innovation in the fields of software applications and analytics, including advancements in machine-learning techniques and algorithms, has allowed people and businesses to leverage so-called Big Data.

3. On the technology adoption curve, the IoT falls somewhere between the innovation phase and early adoption phase (Greengard, 2015). If the technology reaches full maturity and lives up to its potential, the IoT will transform every aspect of our daily lives. Opportunities include the ability to increase employee productivity, improve connectivity, lower operating costs, enhance customer and citizen experiences and boost revenue in many economic sectors (Folk et al., 2015). For an overview of some of the key sectors that stand to profit from the IoT, see Table 1.

Table 1: EXAMPLES OF FUTURE SMART SECTORS
Agriculture
Cities/Urban Management
Counterterrorism
Energy
Firefighting
Food safety
Health Care
Home Management
Law Enforcement
Logistics
Manufacturing (Industrial Internet/Industry 4.0)
Military
Mining
Mobility/Transportation
Shopping

4. The IoT holds enormous potential for good, but challenges and risks are the eternal companions of any disruptive technology. As IoT devices will appear all around us, optimists see a blissful utopia on the horizon that will solve many of humanity's problems. Pessimists see a dystopian future where IoT technologies have been adopted *en masse* without adequate security and with less human and more government and machine control. Neither scenario is very likely at this point, but it is undeniable that the IoT will create technology winners and losers (Greengard, 2015). It is therefore imperative to engage in sustained policy discussions on how to harness the promises and check the perils of the IoT. This report hopes to begin such discussions in a transatlantic security context.

5. The report is part of the Science and Technology Committee's (STC) increasing focus on potentially disruptive technologies, which the Committee pursues through reports, meetings, visits, and other activities (including a 2016 small-scale survey[1]). Moreover, the report builds upon the 2014 STC Special Report on Cyber Space and Euro-Atlantic Security (NATO PA, 2014).

6. First, the report examines the basics of the IoT and its current challenges. Second, it looks at IoT opportunities and challenges for the armed forces. Third, it zooms in on the challenges the IoT creates for critical infrastructure. Finally, it ends with a set of recommendations on the way forward.

II. WHAT IS THE INTERNET OF THINGS?

A. THE BASICS

7. No agreed definition of the IoT exists. As one journalist recently joked about the diversity of views on the IoT, "It's kind of like the three blind men and the elephant parable, but instead of three men, it's 1,000 people touching a sculpture made of wet clay" (Michels, 2017). A good starting point, however, is the definition used by the world's leading information technology research and advisory company, Gartner, which defines the IoT as "the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment" (Gartner, 2017). The IoT is also "a buzz phrase used to describe the computerisation of everything from cars and electricity meters to children's toys, medical devices, and light bulbs" (The Economist, 2017b). Perhaps, the broadest aspiration for the IoT is the so-called 6A Vision: "The goal of the Internet of Things is to enable things to be connected *anytime*, *anyplace*, with *anything* and *anyone* ideally using *any path/network* and *any service*" (Vermesan et al., 2015; Borgia, 2014; rapporteur's emphasis).

8. Outside of academic definitions, the lines between the Internet and the IoT are blurry. Essentially, the IoT "is an umbrella term that refers to anything connected to the Internet" (TechTerms, 2015). When the Internet first emerged, it could be understood as an Internet of computers. Over time, however, the types of connected devices expanded beyond computers and researchers looked for ways to describe this development. The man credited with coining the term IoT was Kevin Ashton, Executive Director of the Auto-ID Center at the Massachusetts Institute of Technology. In 1999, he used the term IoT to describe his vision of future supply chain management based on connecting items with the Internet through radio frequency identification (see below). If car companies could automatically track their inventory of doors, motors and wheels, they could vastly improve their supply chain management. The term has caught on, but even today, companies still compete in coming up with new buzz phrases, such as Cyber-Physical Systems, the Internet of Everything or the Physical Web. Just as the Internet of Computers simply became the Internet in most people's minds, one might suspect that, as the IoT becomes increasingly absorbed into daily life, it will once again become just the Internet.

9. Like the Internet itself, the IoT does not consist of just one technology or one network (Vermesan et al., 2015). Rather, it is made up of "islands of connected devices" (Greengard, 2015). A distinguishing feature of the IoT is a high degree of heterogeneity: Smart lightbulbs that can be dimmed through your smartphone are very different from tagged shipping containers which can be traced worldwide, which are again very different from self-driving cars with enough sensory technology to navigate urban traffic.

10. To get a better picture of what constitutes the IoT, it is helpful to examine its building blocks. At the core of the IoT are "things" that are physical, connected and smart (Folk et al., 2015). Such IoT devices collect, transmit, compute and act upon data, which has been described as the "new

1 For further information, please refer to the STC 2017 General Report, *Maintaining NATO's Technology Edge: Strategic Adaptation and Defence R&D* [174 STC 17 E bis]

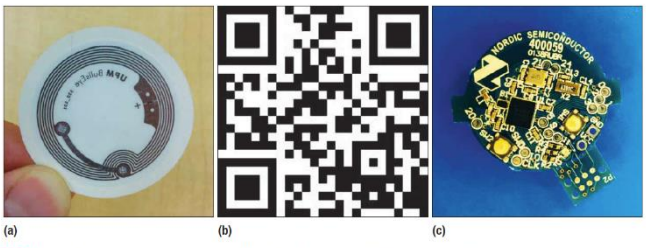
oil" or "new currency" powering today's economies (Vanian, 2016). The seven processes described hereafter tie these things together into the IoT (Al-Fuhaqa et al., 2015).

11. **Identification**: To be part of the IoT, things need to be nameable and addressable – just like computers can be located and identified through their Internet Protocol (IP) addresses. Put differently, smart devices are of no use if they cannot be readily reached. Today, a multitude of identifiers exist for IoT devices, for example Uniform Resource Identifiers, Electronic Product Codes, Ubiquitous Codes and addresses in the latest IP standard (IPv6).

12. **Sensing**: Sensors enable smart things to obtain data and thus interact with the physical world. Today's smartphones for example contain a multitude of sensors. They can contain proximity sensors; light sensors; barometers; magnetometers; sensors for positioning, speed and currents; accelerometers; gyroscopes; thermometers; pedometers; heart rate monitors; fingerprint sensors; and even radiation sensors. Researchers are even working on sensors that can "taste" and "smell" and, in turn, emulate taste and smell for the user.

13. **Communication**: The data collected by sensors needs to be passed on to where they can be analysed and acted upon. Temperatures collected by smart thermostats need to reach the parts of the network where something can be done about them (e.g., turn the heat up, turn on the air conditioner, etc.). A diversity of wired and wireless technologies – all with distinct advantages and disadvantages – can perform such communications. For example, the beginnings of the IoT lay in the use of Radio Frequency Identification (RFID) tags for the nation-wide or global tracking of merchandise. Today, RFID tags can be found on many consumer products. Other tag technologies include Quick Response (QR) Codes and Bluetooth Low Energy (see Figure 1). Other communication technologies include Near-Field Communication (NFC), Wi-Fi, Bluetooth or ZigBee as well as narrow band radio technologies (either based on dedicated services or on mobile phone systems).

Figure 1 (Want et al., 2015)



(a) (b) (c)

FIGURE 2. Various forms of electronic tags support the Physical Web (all about the size of a quarter): (a) a near-field communication (NFC) tag; (b) a quick response (QR) code; and (c) a Bluetooth low energy (BLE) tag. However, it is not clear which technology—each with its own affordances and problems—will become the primary IoT enabler.

14. **Computation**: Once data is collected and communicated, the data needs to be computed. This can again happen in numerous ways. Some IoT devices will be able to process data via micro-controllers. Often, they will also be able to act on the information through actuators. For example, when a family is away on vacation, smart smoke detectors can place an emergency phone call directly to the fire department. Other devices, however, will send their data to smartphones or computers in the vicinity. In yet other configurations, local computer networks could either be able to process the data on their own or act as gateways to cloud computing services.

15. **Services**: Once the data gets where it needs to be, services enter the picture. A smart home system will regulate the temperature, air flow or lighting in a building. A smart logistics system will know when it needs to order new components for the assembly line or give the order to ship a container which has just been filled up. A smart energy grid will analyse the data streaming in from its components and will subsequently optimise energy production or use. Ultimately, the possibilities for IoT services are only limited by human (or machine) imagination.

16. **Semantics**: For several years, researchers have been working on the so-called semantic web "which provides a common framework that allows data to be shared and reused across application, enterprise, and community boundaries" (W3C, 2013). The Semantic Web should integrate and combine data from many heterogeneous sources. This would allow humans or machines to sort through the available data in a more intuitive fashion. Semantics thus becomes extremely valuable in the IoT environment. One expert thus argues that semantics is "the brain of the IoT" (Al-Fuhaqa et al., 2015).

17. Due to its heterogeneity, **IoT infrastructures** can take many forms. Some IoT systems work mostly at the local level. For example, smart homes will largely be self-contained. However, the data gained at one level might be integrated into a larger system. Data from all smart houses in one neighbourhood could be mined for clues on how to better manage all of them. Other systems will primarily work at the macro scale. For example, a system of sensors which is deployed across the globe and collects environmental data could feed directly into analytics of climate change or weather patterns. Some systems will send data to centralised cloud computing services. Others could use local computing capabilities in so-called fog or edge computing systems, which will have less computing power but act faster. A smart traffic light system, which needs to warn pedestrians crossing the street if a car is about to run a red light, cannot afford the time to send its data to the cloud (Bonomi and Natarajan, 2014). It would save lives if the system could draw on local computing in other nearby smart devices (i.e. the fog/edge). Some smart things will talk directly to the cloud; others will talk to the cloud indirectly, for example through the user's tablet computer. IoT systems can also be integrated into systems of systems. Air travel data collected primarily for the purposes of improving passenger flow could be combined with health system data to identify how infectious diseases spread from region to region. Some systems might primarily rest on machine-to-machine communications, without much human interference in day-to-day operations; others will involve plenty of human-to-machine communications. Certain objects are primarily physical objects with IoT elements attached, for example crates of machine parts equipped with RFID tags. Other things will chiefly be digital objects that also exist in the physical world, for example tablet computers. In sum, the possibilities of IoT system architecture appear almost boundless.

B. TECHNICAL AND ENGINEERING CHALLENGES

18. Inevitably, numerous technical and engineering challenges need to be solved before the IoT can truly become ubiquitous. One of the biggest challenges is the need to elaborate **common standards**. Currently, a multitude of standards are being developed, for example by companies. A consolidation of standards, aiming at the adoption of good standards regardless of source, is therefore vital to ensure interoperability. Standardisation organisations and others are therefore working intensely on IoT standards, and alliances between different actors are beginning to join up with the aim of consolidation. Standardisation and interoperability are so critical because the biggest promise of IoT technology lies in the added value of connecting many different IoT devices and using the Big Data they generate. To illustrate, in an urban environment, smart traffic lights and roads or energy and water systems would all provide an added value in themselves. However, the bigger potential for urban management lies in connecting the data from all of them to reduce costs and improve efficiency, quality of life and safety. One analysis even argues that "40% of the potential economic value of the Internet of Things will depend on interoperability" (Baily and Manyika, 2015). Indeed, in June 2015, the Committee saw the possibilities of such complex systems at the New York Police Department's Lower Manhattan Security Initiative, which integrates cameras, sensors, public records and other data sources and provides a real-time or archived picture of New York City (NATO PA, 2015).

19. For the IoT to be adopted broadly, other key technical and engineering questions include (safety, security and privacy questions are discussed in the next sub-section):

- **IoT infrastructure**: As the amounts of smart devices grows, how will they be connected to (parts of) the IoT? Where will the computing take place: in small local networks, in a decentralised fog of devices or in centralised clouds?
- **Context sensing**: Can we develop devices that can sense the context they find themselves in to make better decisions? For example, could a smartphone automatically silence itself when it senses it is in a cinema?
- **Connectivity of low-tech devices**: How do we integrate low-tech IoT devices, for example smart doorknobs, into networks where they will meet high-tech devices with much more computing power?
- **Device discovery**: How will users of the IoT – machines or humans – find IoT devices when there will be billions of them scattered around the globe? Searchable database of IoT devices exist already, but can they be scaled up and made user-friendly?
- **Latency**: How can we ensure that data get to where it needs to be in time to act? For example, could systems in autonomous cars react quickly enough to prevent accidents?
- **Mobility**: How can we ensure that IoT devices integrate effortlessly into the networks they encounter as they move, for example connected cars driving through Europe? What infrastructure investments must governments make to ensure adequate coverage across countries and borders?
- **Scalability**: Can we develop applications that can control many different devices, as it will not be practically feasible to download one app for every small IoT service?
- **Big Data analytics**: How do computing services deal with Big Data, characterised by high volumes, velocity and variety of data from devices often distributed over large areas?
- **Costs**: As devices and services become more complex, can providers keep the costs in check to allow the IoT to be widely adopted?
- **Energy demand**: Can we sustainably manage the energy needs of a mushrooming number of IoT devices?
- **Environmental concerns**: If IoT devices become ubiquitous, what impacts will that have on the management of electronic waste?

20. Researchers, industry and governments realise that these challenges need to be overcome or managed if the IoT revolution is to become a reality and are thus working hard on these problems. A great number of emerging technologies might contribute to solving (some of) these problems and to unlocking the IoT's full potential. Some of these technologies can be found in Table 2.

Table 2: ENABLING TECHNOLOGIES FOR THE IOT
Additive Manufacturing
Advanced Manufacturing Systems
Advanced Materials
Artificial Intelligence
Biotechnology
Block Chains
Complex Data Mining
Nanotechnology
Photonics
Quantum technology
Robotics

C. THE FUTURE OF THE IOT: THE BUSINESS CASE, SECURITY AND PRIVACY

21. How quickly the IoT will become ubiquitous is dependent on a range of factors beyond technical and engineering challenges. While the potential for adaptation in the public sector is enormous, the private sector is moving faster in offering IoT devices and services. The future of the IoT will thus be shaped by commercial providers and consumers.

22. Companies must be convinced of the business case. The added value of the IoT is very clear in many sectors, for example in supply chain management. Large retail corporations like Amazon and Walmart have much to gain by employing the IoT. For other sectors, the case is not as clear. The central question is whether companies can extract enough value from the IoT to make the necessary investments. After all, the IoT is not an end in itself for the companies; they have to see ways to capture market shares and increase profit. Critics already argue that IoT business models are broken, in part because of the lacking functional value of many IoT devices and rising costs (IBM, 2015).

23. Customers also need to be convinced of the added value of IoT devices. If customers are not convinced that a connected toaster enhances their lives, they will not buy it. Other key factors for consumers include reliability and ease of use of IoT products and services. As one group of researchers put it, "we need a way for any user with any smartphone or tablet to walk up to any IoT device and interact with it (without a specialised app)" (Want et al., 2015).

24. As with cyber space in general, big issues surround security and privacy. If providers cannot ensure that IoT devices are secure and protect the privacy of their customers – or if customers do not trust companies on this – the IoT will not be adopted quickly or extensively. Broadly speaking, three categories of risks exist:

- **Privacy risks:** One recent example is the alleged installation of a secret "fake off" mode in certain Samsung smart TVs from 2012 to 2013 by the US Central Intelligence Agency (Calore, 2017). This claim is based on alleged US government documents published by WikiLeaks. These documents suggest that, if the intelligence gathering tool is activated, the TV appears off but could gather audio and possibly video data in its vicinity.
- **Systemic risk:** To illustrate a systemic risk, in 2016, the so-called Mirai botnet consisting of some 145,000 cameras and digital video recorders (DVRs) was used to carry out an attack against a major domain name server, which led to the disruption of a number of major web services and websites. Overall, the attack involved as many as 1 million internet-connected devices (Agawu and Bate, 2016).
- **Wider risks inherent in poorly secured IoT devices:** See the Section IV on Critical Infrastructure and the IoT.

25. IoT networks are difficult to secure. Risks include malfunctioning IoT devices, accidental misuse of devices and targeted attacks (from primitive to sophisticated attacks) (Evans, 2015; Lewis, 2016). A few examples highlight the potential risks:

- When he was US Vice President, Dick Cheney had the wireless capability in his pacemaker disabled, due to concerns that hackers could deliver a fatal shock to his heart (Zetter, 2015).
- In 2015, a viral video demonstrated how hackers can remotely hijack a Jeep's on-board entertainment system and disable the steering wheel and brakes (Valasek and Miller, 2015).
- A 2015 report warned that Wi-Fi networks on airplanes are potentially vulnerable to attacks by hackers who could seize control of planes in mid-flight (Hern and Agencies, 2015).
- In 2017, a German government agency issued a warning on a talking doll. Its smart technology could reveal personal data due to an unsecure Bluetooth device. Hackers could theoretically listen and talk to the child playing with the doll (BBC News, 2017).

26. The Internet is already pervasive, and the wide adoption of IoT will make connectivity almost omnipresent and lead to a high density of information sharing over wired and wireless networks. The fundamental security and privacy issues in the IoT are not much different than the ones faced in the rest of cyber space. One key difference is, however, that many IoT devices are very low-tech in nature and often – at least in the current and medium-term stage of IoT adoption – only come together in ad hoc networks over a short period. Equipping smart light switches, super market shelves or tractors with the same security and privacy standards as computers, smartphones or tablets might not be feasible from an economic standpoint. How then do we ensure adequate protections?

27. Researchers are developing technological solutions for security and privacy protection. Even for low-tech devices, IoT designers are developing so-called system-based security solutions. For example, low-tech devices could connect to the Internet through a more sophisticated controller that carries out the in-depth security that low-cost devices are unable to perform. Also, a new paradigm called data-centric security is gaining support, which is a more pragmatic approach to security, as it recognises that, even with the best cyber security tools in place, intruders will always find a way into your systems (Mullins, 2016). In this approach, the protection of the (most valuable) data itself becomes the highest goal. The defenders thus must understand their data infrastructure, flows and risks; classify sensitive date; and monitor and control the use of data.

28. A key debate in IoT security and privacy protection is whether strong protections should be "baked in" from the beginning or whether the market should take off first and then additional security can be "bolted on" once the IoT market has taken off (Lindsay et al., 2016). For advocates of the former, regulators can avoid some of the faults with the Internet's development, which was originally designed for small-scale networks of trusted computers – not a mass market filled with its cyber criminals. The view that such "security by default" should be the aim of designing devices and services is the most widespread position. However, advocates of the view that additional security can be "bolted on" fear that installing costly security features could choke the nascent market. One expert argues that not every IoT device needs the same high level of security and privacy (Lewis, 2016). He proposes to apply three metrics: the value of data collected, the criticality of the data and the scalability of failure. In other words, protection should be highest if IoT devices and services collect and transmit highly valuable and/or critical data, and/or if failure in one part could cascade into widespread failures.

29. One-hundred percent security is not possible. As one news magazine recently argued, "The risk from fraud, car accidents and the weather can never be eliminated completely either. But societies have developed ways of managing such risk – from government regulation to the use of legal liability and insurance to create incentives for safe behaviour" (The Economist, 2017a). (For one national example of strategic principles, see Table 3.) However, regulators should probably aim for a balanced approach that avoids both a rush to the market and an overcautious tactic. As should become clear in the next section, it also seems prudent to make the more critical parts of the IoT, the IoT of the armed forces and the parts touching critical infrastructure, much more secure than consumer goods.

Table 3 **STRATEGIC PRINCIPLES** **FOR SECURING THE INTERNET OF THINGS** **(US DEPARTMENT OF HOMELAND SECURITY)** **(DHS, 2016b)**
Incorporate Security at the Design Phase
Promote Security Updates and Vulnerability Management
Build on Recognized Security Practices
Prioritize Security Measures according to Potential Impact
Promote Transparency across IoT
Connect Carefully and Deliberately

D. WHAT IS THE ROLE OF NATO AND THE EU

30. Fortunately, most policy makers are taking these challenges seriously. Regarding the IoT, the European Union (EU) for example has engaged in a number of policy initiatives and efforts to utilise its full potential. The EU's IoT vision is based on three main pillars: a single market for the IoT; a thriving IoT ecosystem; and a human-centred IoT approach. In March 2015, the European Commission launched the Alliance for Internet of Things Innovation, an initiative aimed at developing a dynamic IoT ecosystem, boosting innovation and deployment and encouraging interaction among stakeholders. Also in 2015, the Commission adopted the Digital Single Market Strategy, which emphasises the need to avoid fragmentation and foster interoperability in the IoT. Key strategic IoT areas for the EU are smart agriculture, smart cities, smart industries as well as sustainable reverse logistics, smart water management and smart grids. Between 2014 and 2017, the EU is investing EUR 192 million in IoT research and innovation. The ongoing EU Horizon 2020 programme has set up concrete research and innovation objectives for IoT, and the European Commission (EC) has launched a call for proposals on IoT large scale pilots in the areas of wearables, assisted living, connected vehicles, smart cities, smart agriculture and water management. The call has now been closed and the projects have been granted (in total: five large-scale pilot projects and two collaboration and support activities). The EC, together with the Alliance for Internet of Things Innovation, is also currently working on a proposal for new legislation creating a certification process for IoT devices that would ensure users are protected, in other words a set of baseline requirements for security and privacy (European Commission and Alliance for Internet of Things Innovation, 2017). The EC would encourage companies to devise a labelling system for internet-connected devices that are approved and secure (Stupp, 2016).

31. NATO has few activities directly related to the IoT beyond acquiring situational awareness of the topic. However, the Alliance has slowly begun to engage with it. For example, the Information Systems Technology Panel of Science and Technology Organization (STO) supported by the STO's Collaborative Support Office (CSO) launched a three-year task group in 2016 on Military Applications of Internet of Things.[2] The task group aims to demonstrate the military value of IoT through concept trials, to define potential military IoT architecture(s), identify possible risks, mitigations and unsolved challenges of using commercial IoT technology in the armed forces. The task group also aims to create an IoT network across the NATO, EU and national communities.

32. As this report has shown, many challenges remain in terms of securing the IoT. A 2015 survey found that "71% of executives believe that the security needed to secure IoT devices is at least 12 months and as much as 24 months behind the deployment of these devices" (Tripwire, 2015). It is thus critical that Allies strengthen their cyber defence and security policies, in the civilian domain as well as in the armed forces. Efforts to improve critical infrastructure security must also feature highly on this agenda. Fortunately, Allies, NATO as an organisation and the EU take these challenges very seriously. Both NATO and the EU strengthened their policies in this regard in 2016. At the 2016 Warsaw Summit, the Alliance once again strengthened its cyber defence policies. Heads of state and government reaffirmed NATO's defensive mandate, and recognised cyber defence as part of the Alliance's core task of collective defence. Allies also reaffirmed NATO's readiness to invoke Article 5 in response to a significant cyber-attack. The Alliance also went one step further by recognising cyberspace "as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea" (NATO, 2016). In October 2016, NATO signed a Memorandum of Understanding with the 28 Allied cyber defence authorities, which sets out arrangements regarding information exchange, and cyber incident prevention, resilience and response capabilities. For its part, the EU finalised its Directive on Security of Network and Information Systems – its first piece of EU cybersecurity legislation. In

[2] The lead nation is Poland. The participating nations are Belgium, Finland (as a partner nation), Germany, the Netherlands, Romania, the United Kingdom and the United States. The NATO Communications and Information Agency is a participating organization. For more, see here: https://www.cso.nato.int/activity_meta.asp?act=8647.

addition, in February 2016, NATO and the EU signed a Technical Arrangement in order to strengthen cooperation on cyber defence, including in the areas of information exchange, training, research and exercises. It is imperative that this positive policy momentum is retained, as IoT challenges will only grow over time.

III. ARMED FORCES AND THE IOT

33. Historically, the US Department of Defense (DoD) has played a fundamental role in the development of the sensor, computer networking and communications technology that are the foundation of today's IoT (Zheng & Carter, 2015). Alas, military IoT adoption is still in its infancy. However, as the Committee learned during its visit to Leonardo-Finmeccanica in October 2016 (NATO PA, 2017), defence companies and the armed forces are eager to prepare, understand and leverage the IoT (Seffers, 2015). The US Defense Information Systems Agency, for example, argues that the IoT will "result in an explosion of capabilities on our sensitive unclassified and classified networks" (Seffers, 2015). The Agency adds that "From improved logistics tracking to optimised building security and environmental controls to health monitoring of individual soldiers, the Internet of Things will impact everything we do".

A. THE POTENTIAL OF IOT TECHNOLOGIES FOR THE ARMED FORCES

34. Connected devices can benefit today's militaries by increasing efficiency and effectiveness and reducing costs (Zheng & Carter, 2015). Military IoT would facilitate modernisation and perhaps even revolutionise modern warfare. IoT devices and services can collect increasingly complex data and analyse it faster; make use of increased automation; reduce human error; deliver more precise and efficient military capabilities; and reduce personnel costs.

35. The United States, as the world's biggest military power, is leading military IoT adoption and is already incorporating IoT technologies (Zheng & Carter, 2015) in four areas:

- **Sensors**: The US military focuses mainly on the IoT's potential in combat applications and sensors deployed on different Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems. For example, airborne sensor platforms, surveillance satellites, unmanned aerial vehicles (UAV), shipboard and ground stations as well as soldiers in the field gather data which is then communicated to the Distributed Common Ground System. This system ingests and analyses the data and transmits information up and down the chain of command (NATO PA, 2016). Some experts urge the United States to move towards a full combat cloud infrastructure, transitioning away from separate legacy networks to a unified data centre (Wind, 2015).
- **Fire control systems:** End-to-end deployment of networked sensors and digital analytics enable fully automated responses to various threats in real time and delivery of firepower with pinpoint precision. Examples already in use include the US Navy's Aegis Combat system, Predator unmanned aerial vehicles and the Tomahawk Land Attack Missile.
- **Mobile technologies:** The US military has launched pilot programmes to implement mobile technologies for its soldiers and civilians. One example is the NETT Warrior programme, which equips infantry units with modified Samsung Galaxy Note smartphones linked to the data-capable Rifleman Radio. Soldiers in the field can access a range of apps, such as 3D maps, tracking of friendly forces, language translation, and the profiles of high-value targets. However, lack of connectivity, limited functionality and poor user experience remain obstacles to the widespread deployment of these devices.
- **Logistics management:** IoT devices have been adopted in logistics management to track shipments, manage inventories, train and simulate as well as manage smart energy systems (like NATO's Smart Energy initiative (NATO PA, 2013). However, overall deployment is still limited and poorly integrated.

36. There are several gaps and challenges related to the successful development and deployment of IoT technologies within the US military (Zheng & Carter, 2015). Few systems make use of the full IoT potential, from networked sensors to digital analytics and automated responses. In addition, the military has adopted a "stovepipe" approach to IoT technologies, i.e. different branches develop and deploy very different technologies. This makes them difficult to secure, limiting the ability to communicate across systems or create economies of scale and synergies from different types of data. Other experts, however, argue that a holistic approach across the armed forces could become unwieldy, burdensome and, ultimately, counter-productive. Data collection and processing also underperforms, while automation is lacking. There are further limiting factors, such as the lack of connectivity and the necessary network infrastructure to process the amount of data generated by a military IoT. Substantial investments in infrastructure and analytical software would be required to transfer, store and analyse the generated data. Establishing common standards and protocols to ensure interoperability is another challenge.

37. In addition, cultural barriers are an obstacle to the wider adoption of IoT technology across the military (Zheng & Carter, 2015). Senior officials frequently lack sufficient understanding of new technologies and are often hesitant to replace established routines, adopt innovative solutions and apply them to traditional challenges. Many military leaders are reluctant to rely exclusively on technology and to trust machine-to-machine communication. While IoT applications offer long-term savings, the military is often unwilling to invest because of the large upfront acquisition costs and recent budget constraints. Furthermore, military acquisition processes are characterised by a culture of secrecy and politics, an approach which clashes with the private tech sector's comparatively open culture of experimentation and failure (Zheng & Carter, 2015; NATO PA, 2017). Private tech companies are also sometimes less willing to work with the DoD because of limiting intellectual property rights and export controls.

B. RISKS OF IOT APPLICATIONS IN THE MILITARY

38. IoT devices and applications in the military can also constitute significant security risks, especially regarding electronic and cyber warfare (Zheng & Carter, 2015). As armed forces deploy IoT devices and applications, the number of entry points for cyber attackers will only grow. Insider threats and user error are also cause for concern. Furthermore, most IoT technologies rely on wireless communication via radio frequencies and are therefore vulnerable to electronic warfare, including signal jamming and detection of troop positions.

39. Security risks are particularly prevalent in three areas: vehicle safety, healthcare and supply chains (Campbell, 2016). As already shown, hackers can potentially take over and steer vehicles. Vulnerabilities within the military health care system include the remote controlling of health and safety devices such as manipulating drug-infusion pump dosage levels, heart monitors and defibrillators. Military supply chains can also be compromised, as IoT devices consist of components manufactured and assembled from locations around the world. In addition, the risk that adversaries could spread disinformation within Alliance's networks to disrupt processes and operations should not be underestimated. Finally, many devices in the hands of military personnel can provide attackers with valuable data. For example, a smartphone's camera might disclose information about the security of a military outpost.

C. THE MILITARY AND THE COMMERCIAL SECTOR

40. As noted in the previous section, the private sector drives the development and deployment of IoT technologies. To make greater use of IoT possibilities, armed forces will need to adopt new procurement and contracting procedures (Zheng and Carter, 2015; NATO PA, 2017). Starting with areas that are easier to equip with IoT technologies and where commercial products are available could be a good first step. One area in which IoT applications have considerable cost-saving potential is enhanced logistics management, such as condition-based maintenance and the management of fleets, inventories, bases or energy efficiency. Furthermore, to deliver internet

connectivity in remote areas, the military could invest in commercial satellites for military communications. High-altitude communications relays, using UAVs that operate out of weapons range for example, is another promising technology. Armed forces could also investigate the deployment of miniaturised satellites that weigh about 1.33kg (so-called CubeSats) to create capable networking constellations. The military could also focus on developing security overlays for commercial devices and applications. Finally, as already noted, common standards and protocols are needed to enable fast adoption and integration.

41. Commercial IoT technologies are evolving constantly and rapidly. Military acquisitions processes are, however, long and complex. To access innovation, the military must increase collaboration with the private sector (NATO PA, 2017). Experts have suggested a bottom-up approach and have proposed holding open military technology acquisition fairs in Silicon Valley to solicit creative solutions for the military's problems and needs from innovators (Zheng and Carter, 2015). The establishments of test beds dedicated to identify and experiment with technologies that could benefit the military has also been suggested. Furthermore, there have been proposals to adopt agile software development practices used in the private sector and outsourcing data management to commercial providers.

IV. CRITICAL INFRASTRUCTURE AND THE IOT

42. Critical infrastructure facilities and services are assets or systems which are "essential for the maintenance of vital societal functions" (European Commission, 2017). If critical infrastructure is disrupted, damaged or destroyed, the functioning of society would be greatly impaired (NATO PA, 2014). Essential critical infrastructure is typically found in the government, energy, transportation, financial services, food, information, and communications sectors.

43. The digitisation of critical infrastructure processes offers many economic benefits to operators and consumers, but it also opens the door for significant risks. A well-executed cyber-attack on critical infrastructure or even its accidental breakdown could have terrible and potentially deadly consequences. For example, an intentional shutdown or tampering with data could result in power outages leaving entire cities in the dark, affecting hospital generators, toxic water levels and causing a breakdown in communications, preventing emergency response (Nadboy, non-dated). Thus, the link between critical infrastructure protection and the IoT deserves policy makers' particular attention.

44. As the number of IoT devices, systems and services grows, the cyber threat against critical infrastructure – already substantial – will grow considerably. Risks are rising because a) connected devices are increasingly used in the management and servicing of critical infrastructure and b) chances will become higher that critical infrastructure comes into contact with unsecure connected devices and services. In sum, the cyber-attack and cyber-accident surface will increase significantly.

45. The consequences of critical infrastructure providers failing to achieve a sufficient level of cyber security are much greater than in other sectors. Critical infrastructure providers are increasingly interconnected with each other. More importantly, they all intersect with the primary infrastructure of telecommunications and internet networks. Indeed, telecom and IT service providers are believed to be most at risk because they enable all other critical infrastructure. An attack on one critical infrastructure network can therefore have far-reaching consequences for the rest (The Economist, 2016). An important example in this regard is the cyber-attack on Estonia in 2007, which was hitherto unprecedented in terms of scale and focus. It was perpetrated by unknown foreign cyber-attackers, following Estonia's dispute with Russia over the removal of a war memorial. Next to government institutions, all major commercial banks, telecom companies, media outlets, and crucial servers were targeted. The attack did not result in substantial physical or

economic damage, but it gave momentum to a thorough re-examination of the security of Estonia's e-governance services and a push towards increasing security measures.

46. A fundamental component of much critical infrastructure – and therefore a prime target – is an industrial control system (ICS) which includes supervisory control and data acquisition (SCADA) systems and other types of control systems that monitor processes and control flows of information (Simon, 2017). Usually, an ICS is an isolated, air-gapped system not vulnerable to cyber-attacks. Today, more and more ICSs are, however, connected to the internet, which makes them vulnerable to various types of attack (Simon, 2017). In many cases, critical infrastructure relies on old ICS and SCADA systems, lacking the important security controls of modern IT networks.

47. Cyber-attacks through connected objects can have significant physical implications. In 2008, unidentified hackers infiltrated the Baku-Tbilisi-Ceyhan pipeline, which was then thought to be one of the most secure pipelines in the world. They accessed the pipeline's control system through a wireless network and manipulated the systems, resulting in an explosion (Simon, 2017). In 2015 and 2016, Ukraine experienced a series of cyber strikes against its energy and financial infrastructure. Most notably, hackers took down a power grid in Western Ukraine, leaving thousands of people without power and causing the first confirmed blackout resulting from a hack (Polityuk, 2016).

48. Cyber-attacks on critical infrastructure take many shapes and forms. Threats include electronic, radio-frequency and computer-based attacks on the IT components controlling critical infrastructure. Attackers can deploy malware, social engineering, overloading processes, exploiting hardware and software weaknesses, physical attacks and electromagnetic attacks. Examples of attacks include Distributed Denial of Service attacks, Trojans, Structured Query Language injections, Bot-Network attacks and Zero-Day exploits (Castellon and Frinking, 2015). The weakest links in the cyber security chain are often people. For example, the malware Stuxnet which infected the Iranian Natanz nuclear plant in 2010 was able to enter the closed network via USB thumb drives.

49. Critical infrastructure is becoming a popular target for both individual and state-sponsored cyber adversaries (Simon, 2017). For example, the US Department of Homeland Security's (DHS) Industrial Control Systems Cyber Emergency Response Team, responded to 295 cyber incidents involving critical infrastructure in Fiscal Year 2015 – a 20% increase over the previous year. In the critical manufacturing sector, the number nearly doubled to a record 97 incidents, followed by the energy sector with 46 incidents and the water and wastewater systems sector with 25. Other incidents were reported in transportation systems, government facilities, healthcare and communications. Thirty-seven percent of these attacks were spear phishing campaigns (i.e. targeted scams that trick the target into opening malicious content), while network scanning and probing accounted for 11% (DHS, 2016).

50. Critical infrastructure is a high-value target, as disrupting it has significant economic, political and social consequences (Simon, 2017). Actors carrying out such attacks include hackers, cyber criminals, hacktivists, competitors, other nation states and amateurs (Castellon and Frinking, 2015). The skills required to carry out such attacks have become decentralised and more easily accessible.

51. Given the importance of securing critical infrastructure, governments, international organisations and the private sector are working diligently on improving critical infrastructure security. Increasingly effective security systems for critical infrastructure are being developed, such as digital signatures, cryptography, biometric security, firewalls, intrusion-prevention systems and access-control systems (Simon, 2017).

52. Furthermore, cooperation between government and industry is essential in advancing greater cyber security and preventing cyber-attacks. It will be vital to agree on common standards, guidelines, and practices to ensure the protection of critical infrastructure. Increased awareness, advanced threat-detection capabilities, the education and training of employees and improved resilience in the event of a successful attack or accident will also be of great importance.

V. CONCLUSIONS

53. The Vodafone IoT Barometer from July 2016 reveals some astonishing numbers. Of the businesses that responded to the survey, 28% has already deployed IoT technologies, and a full 76% believe that "the IoT will be 'critical' for the future success of any organisation in their sector" (Vodafone, 2016). As Vodafone's Director for IoT, Erik Brenneis, argues "what matters now is not whether a business should adopt IoT, but how" (Vodafone, 2016). In short, the widespread adoption of IoT technologies in the commercial world will take place sooner or later. Innovative local, regional and national governments already have many projects underway or in the pipeline. Advanced armed forces are slowly beginning to realise the advantages of IoT technologies as well.

54. This report, however, has also shown the many challenges the widespread deployment of IoT brings with it. Policy makers, including national parliamentarians, need to start to proactively shape an IoT environment that remains open, innovative and secure. We have to find the right balance. However, a few general guiding principles for IoT policies should be kept in mind by policy makers:

- Regulatory frameworks and other policies looking to shape the IoT environment should find the right balance between making the IoT reliable, secure and private and providing enough incentives for companies to invest in the IoT technologies.
- Standardisation of IoT technologies should be promoted vigorously.
- Funding for IoT research and development should be adequate to enable the large-scale adoption of IoT.
- Government and in particular the armed forces need to reform the way they adapt to emerging technologies, in light of the commercial sector driving many IoT technology developments. Also, they should be prepared to make long-term investments to reap the full benefit of the IoT in the future.
- Governments must also redouble their efforts on cyber defence and security and critical infrastructure protection, given the growing number of IoT devices and services being deployed.

SELECT BIBLIOGRAPHY

(For further information on sources, please contact the Committee Director)

Agawu, Emefa Addo and Laura Bate, *Cybersecurity Awareness Month... Now with Added Facts!*, New America, 2016

Al-Fuhaqa, Ala, et al., "Internet of Things: A Survey on Enabling technologies, Protocols, and Applications", *IEEE Communication Surveys & Tutorials*, vol. 17, no 4, 2015

Baily, Martin Neil and James M. Manyika, *Reassessing the Internet of Things*, Project Syndicate, 2015

BBC News, *German Parents Told to Destroy Cayla Dolls over Hacking Fears*, 17 February 2017

Bonomi, Rodolfo and Preethi Natarajan, "Fog Computing: A Platform for Internet of Things and Analytics", in: Bessis, N and C. Dobre (eds.), *Big Data and Internet of Things: A Roadmap for Smart Environments*, Studies in Computational Intelligence 546, Switzerland: Springer International Publishing, 2014

Borgia, Eleonora, "The Internet of Things Vision: Key Features, Applications and Open Issues", *Computer Communications*, vol. 54, 2014

Calore, Michael, *Worried the CIA Hacked Your Samsung TV? Here's How to Tell*, 7 March 2017

Campbell, Shawn, *"Military Security in the Age of the Internet of Things"*, *Signal*, 1 February 2016,

Castellon, Nicolas and Erik Frinking, *Securing Critical Infrastructures in the Netherlands: Towards a National Testbed*, The Hague Security Delta, 2015

Cisco, *VNI Complete Forecast 2016*, 2016

Collaborative Support Office, *Military Applications of Internet of Things (IST-147)*, undated

DHS, *NCCIC/ICS-CERT Year in Review: FY 2015*, 2016.

DHS, *Strategic Principles for Securing the Internet of Things (IoT): Version 1.0*, 2016

European Commission, Critical Infrastructure, 2017

European Commission and Alliance for Internet of Things Innovation, *Report on Workshop on Security & Privacy in IoT*, 2017

Evans, Dave, *IoT Threat Environment*, Cisco, 2015,

Fischer, Eric A., *The Internet of Things: Frequently Asked Questions*, Washington DC: Congressional Research Service, 2015

Folk, Chris et al., *The Security Implications of the Internet of Things*, AFCEA International Cyber Committee, 2015

Gartner, *Internet of Things*, 2017

Greengard, Samuel, *The Internet of Things*, Cambridge: The MIT Press, 2015.

Hern, Alex and Agencies, "Wi-Fi on Planes Opens Door to In-Flight Hacking, Warns US Watchdog", *The Guardian*, 15 April 2015

Howard, Philip, *Ideas to Retire: A Closed-Platform Internet of Things*, Brookings Institution, 2016

IBM, *Device Democracy: Saving the Future of the Internet of Things*, IBM Institute for Business Value, 2015

Infineon, NXP, ST and ENISA, *Common Position on Cybersecurity*, December 2016

Lewis, James Andrew, *Managing Risk for the Internet of Things*, Center for Strategic and International Studies, 2016

Lindsay, Greg, Beau Woods and Joshua Corman, *Smart Homes and the Internet of Things*, Atlantic Council Issue Brief, 2016

Michels, Dave, "The Future of IoT: Where It's Heading, What to Expect", *Network World*, 30 May 2017

Mullins, Brian, *All Trends Lead to Data-Centric Security*, Digital Guardian, 2016

Nadboy, Michelle, *Industrial Internet Of Things (IoT): Identifying The Vulnerabilities Of Field Devices*, Water Online, non-dated

NATO, *Warsaw Summit Communiqué*, 9 July 2016

NATO PA, STCEES Report, 2013, Osman Askin Bak, *New Energy Ideas for NATO Militaries: Building Accountability, Reducing Demand, Securing Supply*

NATO PA, STC General Report, *Maintaining NATO'S Technology Edge: Strategic Adaptation and Defence Research & Development,* 2017

NATO PA, *Mission Report: Italy, 3-7 October 2016*, 2017

NATO PA, *Mission Report: Connecticut and New York, United States*, 1-4 June 2015
NATO PA, STC Special Report, *Cyber Space and Euro-Atlantic Security*, 2014
NATO PA, STC General Report, 2016, *The Future of Allied Airborne Intelligence, Surveillance and Reconnaissance*,
Polityuk, Pavel, *Ukraine Investigates Suspected Cyber Attack on Kiev Power Grid*, Reuters, 20 December 2016,
Seffers, George I., *"Defense Department Awakens to Internet of Things"*, *Signal*, 1 January 2015
Simon, Tobby, *Critical Infrastructure and the Internet of Things*, Global Commission on Internet Governance, Paper Series, no 46, 2017
Stupp, Catherina, *Commission Plans Cybersecurity Rules for Internet-Connected Machines*, *Euractiv*, 5 October 2016
TechTerms, *Internet of Things*, 2015
The Economist, *Securing the Digital City: Cyber-Threats and Responses*, 2016
The Economist, *The Myth of Cyber-Security*, 8 April 2017a
The Economist, *Why Everything is Hackable*, 8 April 2017b
Tripwire, Enterprise of Things, 2015,
Valasek, Chris and Charlie Miller, *Remote Exploitation of an Unaltered Passenger Vehicle*, Technical White Paper, IOActive
Vanian, Jonathan, "Why Data Is the New Oil", *Fortune*, 1 July 2016
Vermesan, Ovidiu et al., *"Internet of Things beyond the Hype: Research, Innovation and Deployment"*, in: Vermesan, Ovidiu and Peter Friess (eds.), *Internet of Things – From Research and Innovation to Market Deployment*, European Research Cluster on the Internet of Things (IERC), Gistrup: River Publishers, 2015
Vodafone, *Vodafone IoT Barometer 2016*, 2016
W3C, *W3C Semantic Web Activity*, 2013
Want, Roy, Bill N. Schmitt and Scott Jenson, "Enabling the Internet of Things", *Computer*, vol. 48, no. 1, 2015
Wind, *The Internet of Things for Defense*, 2015
Zetter, Kim, "Medical Devices that are Vulnerable to Life-Threatening Hacks", *Wired*, 24 November 2015
Zheng, Denise E., Carter, William A., *"Leveraging the Internet of Things for a More Efficient and Effective Military"*, Center for Strategic and International Studies, 2015