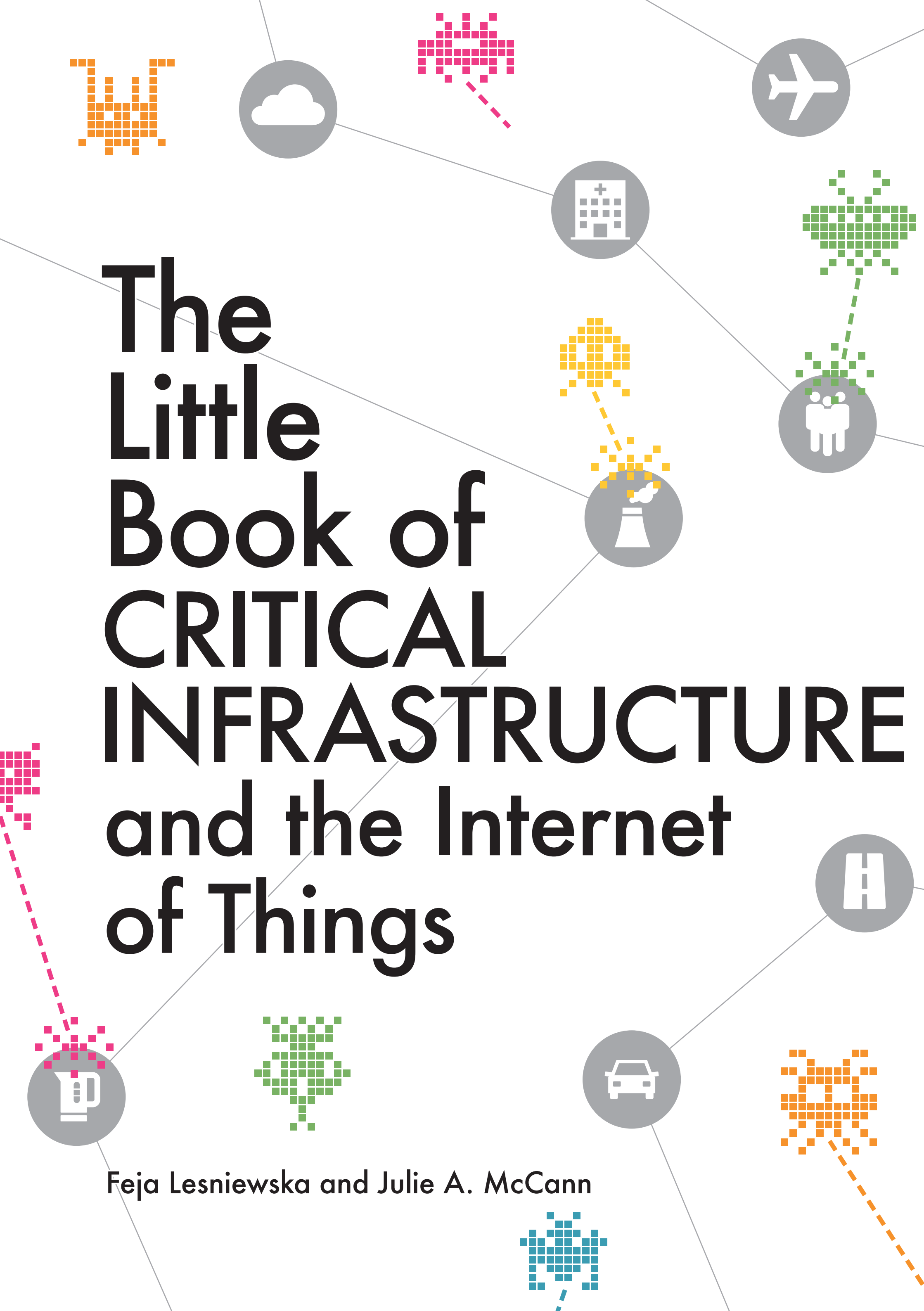


The Little Book of CRITICAL INFRASTRUCTURE and the Internet of Things

Feja Lesniewska and Julie A. McCann

PETRAS
INTERNET OF THINGS
RESEARCH HUB

Editor of the PETRAS Little Books series:

Dr Claire Coulton
ImaginationLancaster, Lancaster University

With design by Michael Stead, Roger Whitham and Rachael Hill
ImaginationLancaster, Lancaster University

imagination
LANCASTER

ISBN 978-1-86220-359-4

© ImaginationLancaster 2019
All rights reserved.

Lancaster
University

The Little Book of CRITICAL INFRASTRUCTURE and the Internet of Things

Feja Lesniewska and Julie A. McCann

About the authors

Dr Feja Lesniewska is a Postdoctoral Research Associate for the EPSRC-funded PETRAS Internet of Things (IoT) Research Hub at STEaPP, University College London. She has published on a range of forest related issues including climate change, energy, certification, illegal trading and human rights. More recently, her research has examined the growing importance of emerging technologies, including the Internet of Things and blockchain, in environmental law and policymaking.

Professor Julie A. McCann is Professor of Computer Systems at Imperial College London. Her research centres on highly decentralised and self-organizing scalable algorithms for spatial computing systems that include wireless sensor networks, cyber-physical systems and the Internet of Things. She leads the Adaptive Embedded Systems Engineering Research Group and directs the cross-Imperial College Centre for Smart Connected Futures. She has been working with Cisco, Intel, NEC and others on substantive smart city and critical infrastructure projects having received significant funding though bodies such as the UK's EPSRC and NERC, as well as various international funds like Singapore's NRF - her Critical Infrastructure work is funded via the Turing Institute. Julie is an elected peer for the EPSRC and BCS Fellow.

Acknowledgements

This book is based on our research conducted for the PETRAS Cybersecurity of the Internet of Things Research Hub funded by the UK Engineering and Physical Sciences Research Council under grant EP/N02334X/1. The aim of PETRAS is to explore critical issues in privacy, ethics, trust, reliability, acceptability, and security and is undertaken by researchers from University College London, Imperial College London, Lancaster University, University of Oxford, University of Warwick, Cardiff University, University of Edinburgh, University of Southampton, University of Surrey, Newcastle University and the University of Bristol.

Contents

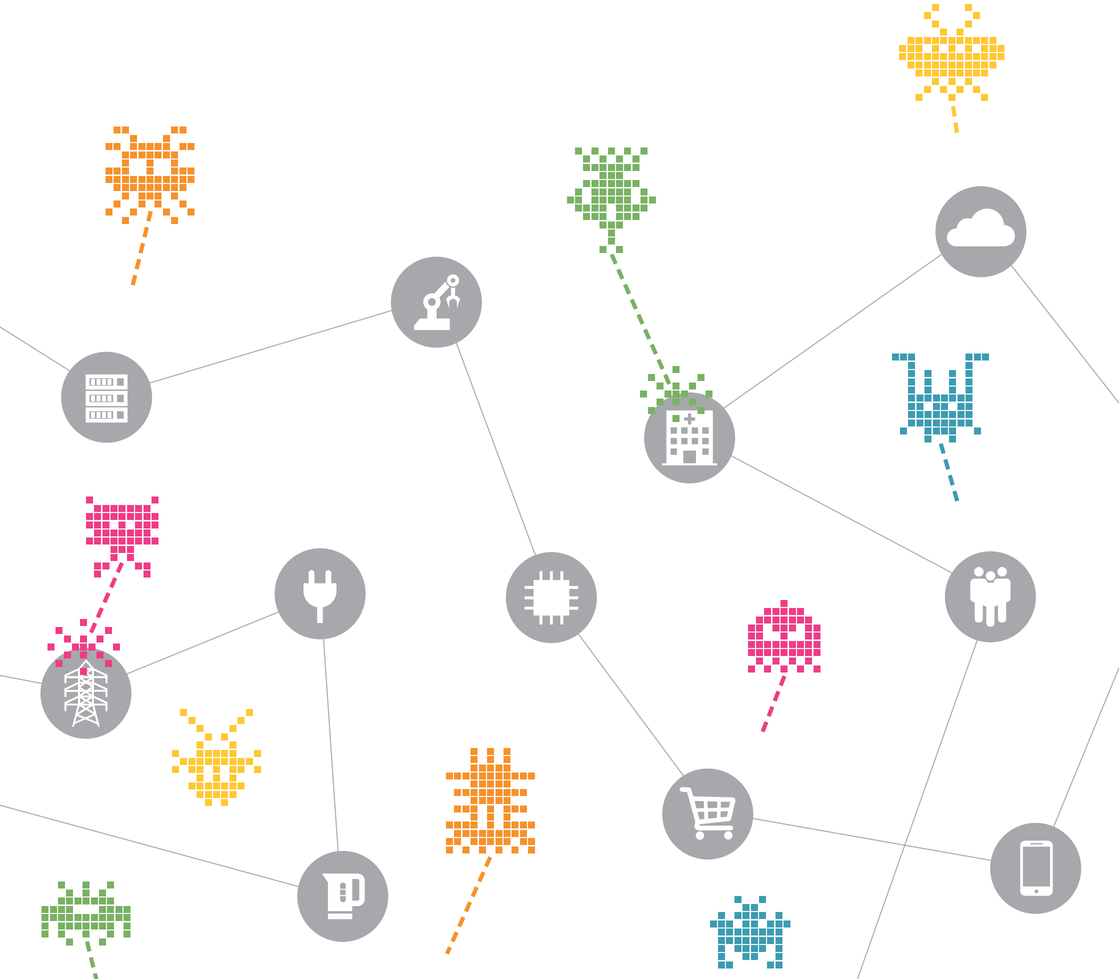
What this little book tells you

This Little Book tells you about the Internet of Things (IoT) and how this is generating changes in the everyday world around us. Using examples taken from the research for the PETRAS project, the Little Book illustrates how the IoT is making us more dependent on new technologies in novel ways and in situations of which many of us are unaware. It reveals how new information and communication technologies (ICTs), such as sensors, data analytics, artificial intelligence and cloud computers, incorporated into critical infrastructures that society depends on for services like health, energy, transport and agriculture, can bring about huge benefits. However, incorporating these new ICTs into critical infrastructure can also result in new risks, some yet unknown, which may threaten the security of society, the environment and human well-being. This Little Book surveys how governments, as well as businesses, are designing and using new policy tools and processes to reduce these risks so that societies that are becoming increasingly reliant on IoT-dependent critical infrastructure are safe, secure and sustainable.

This book has been organised into three parts. In the first, we begin by *defining what we mean by critical infrastructure and how it can benefit societies around the world. We also discuss how we also consider the natural environment as a critical infrastructure*. In this section, we focus on how advances in ICTs like satellite global positioning systems (GPS), sensors with Radio-Frequency Identification (RFID) and artificial intelligence (AI), offer new possibilities for critical infrastructure design and development.

In part two, we *define what we mean by the Internet of Things and explain how it functions within critical infrastructures*. Using examples from water management and precision agriculture, we highlight the potential benefits. We also focus on the vulnerabilities of IoT systems and the impact this can have on critical infrastructure.

In the final part, we take you through some of the *policy and regulatory initiatives that countries like China and the United States, as well as the European Union,* have developed to reduce IoT related risks to critical infrastructure. We particularly focus on the policies targeting risks to national security as countries try to protect citizens, the environment and the wider economy. We also examine several private sector measures to improve IoT critical infrastructure systems' security.



Part One

Infrastructure: What is it and why is it important?

Every human society from the Aztecs to the Greeks to the Victorians has designed, built and maintained infrastructure to harness energy, transport people, deliver services and move goods, especially from farms to towns and cities. Familiar structures to us, such as roads, aqueducts, bridges, airports, ports, train stations, waste treatment plants, power stations, hospitals, public buildings and communication facilities are all forms of infrastructure. So, whether we realise it or not, we are surrounded by infrastructure and many might argue that human civilisation is essentially infrastructure dependent. Without it our lives would lack water supplies, sanitation, reliable transport on land, sea and by air, as well as access to constant energy.

Yet a society's infrastructure landscape is always changing. Infrastructure is, after all, just a concept that is shaped by the available technologies. When technologies evolve innovations in infrastructure soon follow. Let's consider the invention of the steam engine, which heralded the beginning of railway infrastructure. This was not only limited to building railway lines. Physical infrastructure including stations, signalling and carriages also needed to be designed and built. They needed to be standardised to some degree so they would all work together safely, efficiently and reliably to deliver the new service of rail travel to a new type of consumer, rail travel passengers. New jobs were created which required people to be educated and trained in new skills. New infrastructures also bring with them cultural change. For example, new words came into common usage, like 'locomotive', and old ones were repurposed, like 'carriage' which previously referred only to horse-drawn transport via roads. Over time, people were also socialised via advertising campaigns and public education initiatives to understand how to benefit from the new technological opportunities. New laws are often required to identify and delegate the responsibilities for delivering and operating the new infrastructure for the benefit of society. Deciding on what rules and values should shape the laws governing new infrastructures becomes a political issue for society that will often have to be debated time and time again as the technologies used to deliver the system evolve such as moving from steam powered locomotive engines to diesel.

The next phase: Critical Infrastructure

Today we live in a time when advances in ICT open up new possibilities to transform our physical infrastructure once again. Until recently, most infrastructures operated in relative isolation. They were physically separate with perhaps only telecommunications including the internet linking them. New ICT technologies like the IoT, AI and big data analytics are providing innovative opportunities to make existing physical infrastructures for energy; water and transport operate within much more interconnected systems.

New cyber ICTs - IoT, AI and big data analytics - are adding a new dimension to our existing infrastructure. In a short space of time, our physical infrastructure will increasingly be dependent on these technologies to operate safely and reliably. This exciting development is turning separate physical infrastructures like roads, hospitals, railways, and ports into critical interconnected systems that are more interactive and responsive to individual needs. This is what we mean by the term, *critical infrastructure*.

These new ICT technologies combined make it possible to gather data from objects such as electrical goods like fridges, which is then transmitted and processed. It is then communicated back to a customer or a device in rapid time to help make decisions about when they might want to buy their energy. For example, it is now possible to distribute electricity using *smart grids* that use digital technology that allow for two-way communication between the energy company and its customers. Smart grids use established grid infrastructure, like pylons, with innovative technologies, like smart meters, to more effectively monitor energy use by households and communicate information. Customers can make more informed decisions to plan their energy use to take advantage of times when tariffs are low, for example setting the washing machine to go on during the night. This can help customers to reduce bills and help companies to manage the pressures on energy demand more effectively by incentivising consumers to take advantage of off-peak pricing offers.

Cultural transformations that happen with changes in infrastructure have not only had far-reaching social and economic impacts but have often resulted in negative environmental impacts too. Petrol and electricity are good examples. Both these technological developments and their associated infrastructure drove immense transformations in the world's economic and social culture. The move to petrol powered transport, brought with it the 'Age of the Automobile' with the associated ideals of personal freedom, democracy and speed. Electrical power was made available to many people in their own homes, at work and in public spaces such as theatres, schools and hospitals bringing advances in leisure, education and health because of investment in coal fired power stations, pylons and cable technology. However, both these technological developments and their associated infrastructure have contributed significantly to rises in greenhouse gas emissions causing climate change and air pollution in major cities around the world. We now live at a time when transitioning away from this fossil fuel dependent transport and energy infrastructure is a global priority. As a result, the physical infrastructure around us is changing. Around us solar and wind powered energy infrastructure are being built and cars powered by electricity, biofuels and hydrogen are becoming more common on our roads.

The environmental and climate change pressures are also making us rethink what the boundaries of critical infrastructure really are. When focusing on critical infrastructure it is usual to only discuss infrastructure designed and built by humans. Yet science has shown us that the Earth's ecosystems; air, water, soil, forests, oceans, and species habitats, are the most important critical infrastructure that humans rely on. Healthy ecosystems are fundamental to the existence of the human race and all other species. Without a healthy, well-balanced environment, most forms of human civilisation will not be able to survive. These *critical ecosystem infrastructures* need to be invested in and cared for.

If we do not take the opportunity to ensure that this next generation in *critical infrastructure* development is *environmentally sustainable* then we will not be able to meet international commitments to tackle climate change under the 2015 United Nations Paris Agreement and the transition to a low carbon sustainable future that all generations can benefit from will not take place. The IoT will play an important role in making this happen. Vital data to help inform those managing natural resources is increasingly available because of the widespread adoption of IoT to observe, monitor, track and process data about the Earth's ecosystems. Not only can resources be used more efficiently but also, waste can be reduced when those responsible for managing them have the information in real time to make informed decisions. This radical transformation, though, needs to be managed so that society undergoes the transition that these changes bring safely, securely and to the benefit of all. Recognising new boundaries when defining critical infrastructure to include ecosystems will help us to achieve this transformation.

From this discussion, we can see the radical transformation taking place as emerging ICTs are turning isolated, physical infrastructures into interconnected systems, which we now know as *critical infrastructure*. We have also highlighted the importance of recognising and working sustainably with the Earth's own critical ecosystems infrastructure using ICT in sectors like farming, forestry, water management and fisheries will be key to humanity's and many other species survival.

Now we will move forward to a more detailed introduction to the IoT. By using several case studies we illustrate how using IoT in existing infrastructure, like water management, as well as production systems like agriculture, new opportunities arise to improve performance, productivity and safety. By making this transition to depend on IoT in our critical infrastructures new concerns about security are raised.

Part Two

What is the Internet of Things?

The IoT refers to objects or things that can be interconnected via the Internet, making them readable, recognizable, locatable, addressable, and/or controllable by computers. The things themselves can be anything: there is no limit on what could be an IoT thing. Anything that is connected to the Internet, or communicate over non-Internet protocols to deliver data, is arguably part of the IoT. The IoT is distinct because it is the 'things' themselves that generate data rather than people. Given that computers and machines are often quicker and more accurate than people when it comes to data gathering and processing, this means that the IoT offers significant data gathering opportunities. In terms of the automation of critical infrastructures, this may also mean that the things can make control decisions and effect actuators such as valves etc.

The term *Internet of Things* (IoT) was coined by Kevin Ashton in the 1990s. He had used sensors to gather data that could be shared across a company's computer network, to help simplify their supply chain. He called these data-enabled parts of the supply chain the 'Internet of Things' and the phrase caught on.

To fully understand the IoT, it is important to appreciate there is much more to it than just the 'things' that are visible to you; other elements exert significant influence in the IoT, but these are often forgotten. Any given device is actually part of a much more expansive and complicated IoT system. What the IoT really represents, and how it works, actually goes way beyond the mere devices. We call these interrelated collections of objects (AI, data stores, 3rd parties, business models, and so on) *IoT constellations*. The IoT is defined by lots of different interrelated factors that are more or less relevant according to the critical infrastructure systems it is embedded in. The IoT is now much bigger than what Ashton originally intended. He was mainly interested in how businesses could become more efficient using the IoT in factories, manufacturing plants, and supply chains, but the usage of the term has expanded rapidly to cover a variety of areas including critical infrastructure. So now, let's take a look at how IoT is being used in infrastructure.

How is the IoT being used in Critical Infrastructure?

We are seeing that these *IoT constellations* are becoming a transformational force in managing and maintaining infrastructure from transport to energy to agriculture. *IoT constellations* – combining sensing instrumentation, actuation and a spectrum of data analytics - cannot only improve and protect critical infrastructure ecosystems, such as water management, but also permit more *joined-up thinking* about how such assets interact and influence upon each other across that entire ecosystem. Water is a good example to illustrate what we mean by a joined up thinking and how it works.

Water supply and the IoT

Water security is currently a hot topic. Water demands are not being met in many regions of the world, where climate change and economic water scarcity (where a country is unable to build or maintain a water distribution network to continuously meet demands) are playing a significant part. This is not a concern for developing countries alone - California in the USA has had severe water restrictions in place for some time, nor is it a problem for countries with hot climates, the UK experienced its wettest drought in 2012, where rain levels were hitting up to 40mm and yet a hosepipe ban prevailed. The reason for this was a combination of dry seasons preceding the wet spell, and the water distribution systems' inefficiency with leakage being the greatest concern. An accident, breakdown or damage of the water infrastructure, can even risk the lives of many people.

Today, water distribution networks are under tremendous pressure owing to growing water demand, ageing infrastructure, poor maintenance and leakage, which can cause:

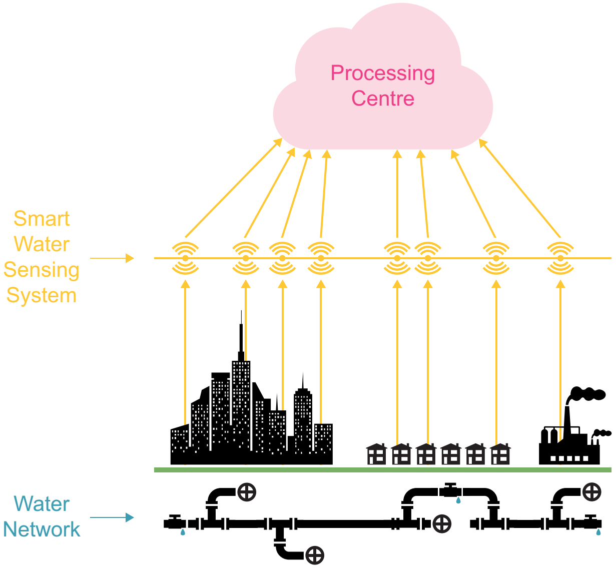
- The quality of water in the system to deteriorate below standards required under law;
- Pressure surges due to intermittent water supply which cause pipe bursts and;
- Leakages which, again, increases the possibility of contamination affecting water quality and putting peoples' health at risk.

Despite the £7.5bn investment in UK water distribution networks, 3.3bn litres of water were lost per day in 2010.

It is due to the increasing incorporation of IoT into water management that the next generation of water networks will not be passive water deliverers. They will be active, highly-distributed control systems that route water intelligently to match demand and route around failures. Real time monitoring and modelling for hydraulics and water quality in water distribution networks has been seen as a way to achieve improved water conservation, localisation of pipe burst and leaks, contamination warning, pump operation optimisation and flow-control. Such systems, enabled by better software, and technology based management strategies, allow informed decision-making and improved service levels. There are numerous research activities examining IoT and other ICTs for the water sector. For example, the Smart Water Networks forum (SWAN) is a global advocate for the role IoT must play in resolving technological challenges related to the monitoring and sustainability of water.

As can be seen in the below image, an IoT based system will rely heavily on sensing and actuation and will effect a dual control system of a water distribution network coupled with a smart distributed sensor/actuator network to monitor the status of the water network and detect leakage or water bursts closer to real-time and then automatically switch the water flows to redirect away from leaking sections, or to increase flow for more demand. The reliability and resilience to cyberattacks on IoT-dependent water systems is of utmost importance - the water network should not be hackable.

The two main problems water companies face is the need to improve the quality of their service and to increase the lifetime of their water pipes. To date, they have not really shown concern about transport infrastructures, and, transport companies have not been concerned with the water



infrastructure. However, given IoT technology and additional data being shared between them, each system can inform the other and allow for more environmentally aware decision making and, therefore, optimal operation at all scales in both infrastructure networks. Put simply, we can imagine a future where the water network sensors detect a leak and the system takes measures to get road traffic automatically rerouted to avoid the leak, thus preventing unnecessary road congestion. Better still, the water network predicts a leak and arranges its repair to fit in with other city maintenance activities. In this scenario, communication systems between different IoT constellations begin to maximise the benefits across critical infrastructure systems through more effective decision-making and coordination. Infrastructure interdependencies (both positive and negative) need to be understood at a system-of-systems level in order to realise these benefits.

As outlined in Part One, we are entering a new era in infrastructure management and maintenance because of innovations in ICT. The rapid uptake of IoT technologies by businesses and governments is due to their potential to drive cost savings, improve asset utilisation and protection, and enhance process efficiencies within a range of service sectors including banking, healthcare, energy and transport. They could boost critical infrastructure productivity as better and more detailed ‘live’ information helps operators and users to make better decisions. In turn, new and improved business models will be developed to deliver new services and capitalise on additional revenue opportunities. The technologies to establish IoT constellations are reducing in cost but also improving in quality. Sensor technologies are able to gather data samples faster, processors can handle larger volumes of information and wireless technologies are covering wider areas using much less energy. However, to achieve the reliable and secure control needed for critical infrastructure services ecosystems like those in transport and agriculture, there remains many data science challenges.

Challenges and vulnerabilities

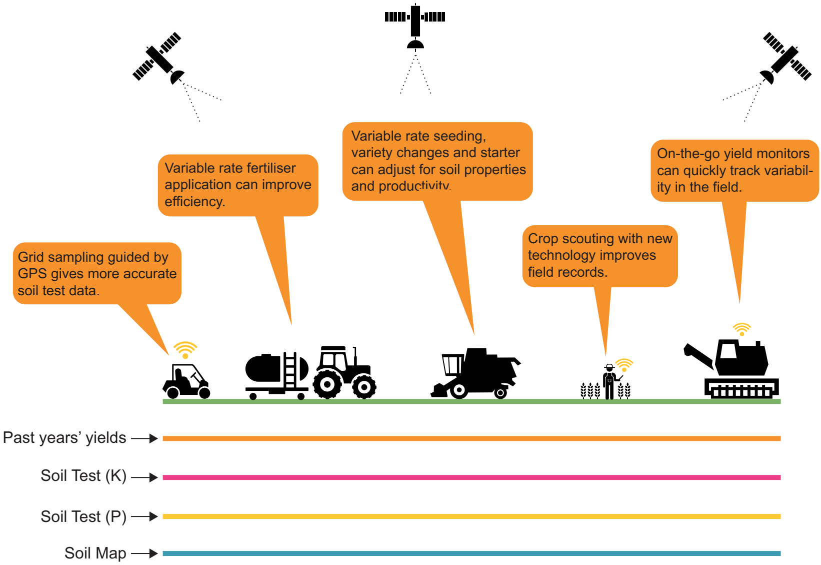
As we have discussed above, the role of IoT in infrastructure and critical infrastructure is likely to be highly beneficial. However, given the predicted importance of the IoT for such critical infrastructures, the security and reliability of IoT systems is much less mature than that of more traditional computing already incorporated into functional systems. One of the primary challenges to be overcome is one of scale. For example, to install an IoT constellation of devices, sensors and data processors at scale for critical infrastructure like a water management ecosystem means that the unit cost of all devices needs not only to be commercially viable, but also easily replaceable, and with continuity of supply, so the system can be maintained.

A solution to the problem of scale and volumes of data needing to be collected, transported, stored and processed is *Fog Computing*. Fog Computing is where highly-distributed data analytics services are made available on Edge devices to either reduce the data to be sent, to collaborate with other Edge devices, to analyse data locally, perform data concentration, or to carry out autonomous actions local to that device (for example to adjust a valve, trip a switch which may be a time-critical action).

The data science and control problems concerning potentially thousands of small devices requires a new understanding of extremely distributed computation operating at many varied scales. Sensing phenomena from an infrastructure using a distributed IoT based system over a large area is one thing, controlling that infrastructure from the same IoT system brings additional challenges. Performing a control function is very difficult to achieve in a distributed way as some decisions made in one locality can affect another. If these are unbounded, this could cause system-wide instability. Indeed, given the ideal is to manage different infrastructures (a whole ecosystem), any errors in one IoT system can permeate to the other IoT systems. For example, for a smart water network, a valve could be activated to react to sudden demand in one area, and if unchecked could mean other areas will not get enough pressure to deliver water to them. The following case study of precision farming illustrates more of the challenges ahead.

Precision Farming

The world faces serious agricultural challenges as the human population rises from today's 7.3 billion to an estimated 9.7 billion in 2050. The UN Food and Agriculture Organisation predicts worldwide food production needs to increase by 70 percent to meet the rising demand. Increasing production is not straightforward but one part of the solution is likely to be precision farming made smarter by using the IoT. The image below shows how precision farming methods might be used.



Variable rate seeding, variety changes and starter can adjust for soil properties and productivity.
Variable rate fertiliser application can improve efficiency.
On-the-go yield monitors can quickly track variability in the field.
Crop scouting with new technology improves field records.
Grid sampling guided by GPS gives more accurate soil test data.
Past years' yields
Soil Test (K)
Soil Test (P)
Soil Map

Precision farming is one area that illustrates the impact one infrastructure (farm) has on a broader ecosystem and how IoT can contribute to making these more sustainable. Generally, precision farming makes use of observation, measurement and decision support to match crop growth behaviours to topological terrain characteristics and then tailor a response to this to optimise the agricultural processes. Most of the focus thus far has been on the dynamic water systems of farmers' fields. For example, GPS-guided tractors and harvesters can more precisely carry out electromagnetic soil mapping, yield data collection and drainage levels. This data shows where one position of the field holds water well and indicates where crops can be more densely planted. For areas of the field where the soil stores less water, it will indicate that more irrigation is required. An example of where this technology has been put to use effectively is the Gallo winery in California. They reduced water usage by 16% while increasing grape yield by nearly a third with an individualised irrigation plan for each block of vines. Working with IBM they used sensors, satellite imagery and weather forecasts to enable the irrigation system to update its schedule as conditions changed.

The global precision agriculture market reached a market value of US$ 4.8 billion in 2017. However, with lower cost sensor technologies, coupled with remote satellite imaging, highly accurate understanding of plant growth, the microbiomes in the immediacy of the plant and its microclimate, farmers using IoT technology can now produce a wealth of information to essentially automate the whole farm. The data captured informs actuation technologies such as automatic feeders on tractors, remote controlled valves, autonomous tractors, and, using geolocation, drones to tailor feed, hydrate, and administer pesticides. This means farmers do not have to waste resources and cause unnecessary pollution, through over-provisioning of water, food and chemicals. There has been research on IoT systems and control systems to optimise pesticide scheduling over a season of 120 days. This helps reduce the use and costs of chemicals, due to more effective application during identified at-risk periods.

Lowering costs is one advantage of this and there are predictions that the global precision farming market is expected to reach $10 billion market value by 2023. More importantly lowering water usage in areas of shortage positively affects whole communities beyond the farm (70% of freshwater is used for agriculture), and lowering the use of pesticides and antibiotics.

Despite these benefits, there are major threats to the uptake and deployment of precision agriculture systems; these fall into two categories:

1. *Technical reliability* – the design of precision agricultural technology needs to consider various natural processes occurring on the farm, its wildlife, dynamic environmental conditions, weather patterns and other actions that would cause disruption to the operation of IoT constellations. For example, temperature differences and other environmental conditions affect the system's' ability to sense and send accurate and reliable data to processors.
2. *Farmer acceptance* – farmers do not want to be locked into a solution that becomes more costly over time. Farmers need an IoT precision system that is easy to set-up so they can be confident that it will operate effectively and be easy to maintain. More importantly, privacy is key to farmers' willingness to adopt these new systems. A recent study found that 81% of Danish and 78% of American farmers mention data ownership as a real concern with indications that there was not much trust in sharing data outside the farm - this despite full knowledge of the potential benefits from exchanging data (e.g. disease movement trending etc.) at regional levels. Data security and privacy are common concerns of those using IoT, from governments to businesses to consumers, so it is no surprise that farmers are equally anxious.

The IoT is causing widespread change across key service infrastructures that we all depend on in our daily lives. The availability of smart, small devices that we have referred to in this section is driving this transformation. As our two examples of water and agriculture illustrate, IoT-dependant critical infrastructure has new security vulnerabilities. Given the predicted importance of the IoT for such critical infrastructures, the security and reliability of IoT systems is much less mature than that of more traditional computing already incorporated into functional systems. This is a worry as more people become reliant on the systems. For example, in 2015 the Ukraine power grid suffered a cyber-attack that disrupted electricity supply, widely believed to be orchestrated by Russia, across three distribution companies. The loss of power to households, services and producers impacted not only the economy but also the wellbeing of the Ukrainian people.

Researchers and companies worldwide are collaborating to ensure such systems behave as they should from a computational perspective. Research Hubs such as PETRAS specifically examine the security landscape of these systems and the policies being designed to reduce risks. Other related projects such as the cross-UK Science for Sensor Systems Software (S4) programme or the Data Centric Engineering programme in the Alan Turing Institute are both addressing guaranteed reliability and engineering of IoT systems to support large critical infrastructures. Yet, technical security schemes cannot solve the problems with IoT and security on their own. Lawyers and policy makers have an important role to play in reforming the rules and standards to make society safe, secure and predictable.

This section has outlined what the IoT is and how it can contribute to delivering a much more integrated, efficient and reliable critical infrastructure. Using examples from water and precision agriculture, we have shown that there are advantages to be gained from embedding IoT into our infrastructure but this introduces new security vulnerabilities, which can be taken advantage of by rogue individuals, groups or states. In Part 3 we take a look at how governments and businesses are trying to address the IoT security problems for critical infrastructure through various policies and measures.

Part Three

If the benefits from incorporating IoT into critical infrastructure are not to be lost due to breakdowns and cybersecurity failures, action is needed to create the rules for our new digital culture. As with previous technological changes, a new rules-based framework is needed to prevent negative outcomes. We have seen this before with railways, automobiles and nuclear power infrastructure, which all needed new laws to be passed by governments to ensure the safety and security of citizens, for example speed limits on roads, seat belts for car passengers and laws on nuclear waste disposal.

There are many ways to reduce the risks and improve the security of critical infrastructure that use extensive IoT systems. Existing laws and policies can be revised, and new standards and guidelines adopted in different sectors to change peoples' and companies' behaviour. Here, in Part Three, we will discuss several case studies to look at how the law and new measures, such as standards adopted by certain sectors, can help to reduce the security vulnerabilities of IoT-dependent critical infrastructure.

National Laws and Regulation

The link between critical infrastructure and national security has made governments around the world introduce laws to make service providers responsible for making their IoT-dependent systems safe, secure and reliable.

The United States was the first country in the 21st century to develop a comprehensive law on national critical infrastructure. This came after terrorists hijacked two commercial airplanes and used them to attack the Twin Towers of the World Trade Centre in New York in September 2001.

The USA Patriot Act of 2001 (42 U.S.C. 5195c(e)) provided a legal definition of critical infrastructure:

> *"critical infrastructure" is defined - referring to "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets*

> *would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."*

In 2009, the US President, Barack Obama, updated the National Infrastructure Protection Plan (NIPP). The plan identified 16 critical infrastructures in the United States that met this definition. These include:

1. the chemical industry;
2. commercial facilities;
3. communications facilities;
4. critical manufacturing;
5. defence industrial bases;
6. the emergency services;
7. the energy sector;
8. financial services;
9. government facilities;
10. healthcare and public health services and facilities;
11. information technology;
12. nuclear reactors;
13. materials;
14. waste,
15. transport systems;
16. water supply and the wastewater system

Meanwhile, to improve the security of critical infrastructure the European Union (EU) member states have adapted existing policies and regulations as digital technologies have evolved. Now, in the EU, there are several main regulatory frameworks that apply to aspects of IoT security. These include the following:

- *European Critical Infrastructure (ECI) Protection Directive* was adopted in 2008 for energy and transport.
- *European Networks and Information Systems (NIS) Directive* adopted on the 6 July 2016 specifies legal standards for digital service providers and operators of essential services in critical sectors such as energy, water management, transport, banking and financial market infrastructures.

Currently, there are 89 ECIs designated, primarily in the energy sector, under the 2008 Directive. Reforms are aiming to expand the ECI to include ICT sectors in the list of Europe's critical infrastructure. This should broaden the scope of the Directive to cover IoT related technologies. The 2016 NIS Directive tackles cyber security risks by involving Operators of Essential Services and Digital Service Providers.

One further development in Europe is the formation of a specialised agency to look into how cyber risks can best be dealt with. The NIS Directive established the European Union Agency for Network and Information Security (ENISA) as the Cybersecurity Agency of the EU. ENISA is helping to design a voluntary cybersecurity certification scheme, aimed at harmonising the procedures and instruments for testing and showing conformity with a responsible level of cybersecurity. In 2017, it produced Baseline Security Recommendations for Internet of Things in the context of critical information infrastructures to inform the governance by both public and private operators in the EU.

China has only recently adopted laws and policies to protect its critical infrastructure. It recently issued draft Regulations on the Protection of Critical Information Infrastructure. This is part of the wider Cyber Security Law coming into effect on 1 June 2017. Critical infrastructure remains undefined in the draft Regulations however; Article 31 of the Cyber Security Law provides a non-exhaustive list of selected critical industries and areas whose information infrastructure would be regarded as critical information infrastructure, including public communications, information services, energy, transport, water conservancy, finance, public services, and e-governance. The draft Regulations require security assessments to be conducted in accordance with the Measures on Security Assessment relating to Export of Personal Information and Important Data. The Cyberspace Administration of China is given the powers to establish a cyber-security incident monitoring, early warning and information reporting system and establish a Critical Information Infrastructure cyber security information sharing system for the purposes of sharing of "network security information" (Article 38). China's focus on information demonstrates how the government links the task of addressing critical infrastructure protection with national data security.

These three examples of two countries and the EU demonstrate the high priority that protecting critical infrastructure is gaining. As technology develops, especially with the IoT, recent laws may have to be revised to address new issues, new threats and new risks. The private sector is often at the forefront of trying to find solutions to emerging technologies because of their commercial value. For example, ensuring that there are standards that all companies respect can be beneficial to the private sector as it levels the playing field in terms of competition. Below, we examine several initiatives by the private sector to improve security for critical infrastructure in light of IoT developments.

Private sector initiatives: Ports, IoT and Security: A voluntary approach

Ports are increasingly depending on digital technologies to operate. As a result, they are becoming more vulnerable to security threats. These can come from corrupt employees, criminals, terrorists, or other hostile sources using a variety of techniques or exploits, such as denial-of-service attacks and malicious software. By exploiting vulnerabilities in ICTs supporting port operations, cyberattacks can potentially disrupt the flow of commerce, endanger public safety, and facilitate the theft of valuable cargo. In 2017, more than 80% of world trade travelled through ports en route to their final destination. Supply chains for many businesses depend on the reliable, secure and safe movement of goods via ports so any disruption can have significant economic impacts for businesses and consumers alike.

In 2018, ports in Barcelona and San Diego were disrupted by cyber-attacks for several days leading to economic and physical losses for traders and operators. In 2017, the International Maritime Organisation (IMO) had drafted the Guidelines on Maritime Cyber Risk Management to improve cyber security practice in the sector. However, this applies largely to cyber security for on-board vessels systems rather than ports. The IMO has taken cyber security seriously, as the number of attacks began to increase. One example was in October 2013 when the Belgium port of Antwerp was hacked. South American drug traffickers had paid hackers to break into the systems controlling the movement of containers through the port. However, the initial attack had occurred in June 2011, meaning that for over two years the security of the container management system had been breached. Traffickers hid drugs in containers shipped from South America and then arranged for them to be illegally removed from the port before the legitimate owner or shipper arrived to collect them. In response to events like this one, ship owners and managers have until 2021 to incorporate the IMO guidelines into practice. Meanwhile the Institution of Engineering and Technology, working in partnership with the UK Department of Transport, simultaneously published a Code of Practice on the Cybersecurity of Ports and Ports Systems.

Different sectors are working to develop *guidance and standards*. For example the GSM Association (who represent the interests of mobile operators worldwide) in November 2016 published an IoT Security Guidelines Overview Document. In addition, leading international technical bodies are working to make information available at one-stop shop style websites. For example, the Institute of Electrical and Electronics Engineers (IEEE) launched the Internet of Things Initiative in 2014, as a single resource for "IoT" information, articles, conferences, training to help build capacity across the technical communities to improve cyber awareness and skills.

Governments also work with businesses to encourage changes in practices. One initiative is the UK government's Secure by Design, which is a code of practice for consumer IoT for smart devices that are to be used in the home (2018, UK Government). This is a voluntary code but one that can lay the foundations for improved practice across sectors developing consumer IoT devices.

This section has highlighted how governments and business representatives are trying to develop new rules and practices so that critical infrastructure relying on ICT can be made secure, safe and reliable. Creating a safe, secure cyber environment for critical infrastructure needs as much investment in education and awareness raising as in the technical and legal issues. The burden for creating a secure IoT world is not shared equally. Business and governments have a bigger role to play but employees, citizens and consumers will have to adapt to a new critical infrastructure culture that is being shaped by emerging technologies like the IoT.

Summary

The IoT is changing the infrastructure we depend on around us. It is anticipated that the widespread adoption of IoT in critical infrastructure systems will bring many benefits to society all around the world including addressing climate change and meeting the UN Sustainable Development Goals.

As this Little Book has illustrated, the IoT is already bringing new opportunities for different critical infrastructure sectors including water and precision agriculture. The new opportunities are driving investments into research and development to achieve the necessary technological breakthroughs needed to overcome obstacles that prevent an IoT system's smooth introduction and safe operation - including the security of the systems they support. However, there is a long way to go from the lab to commercially viable, safe, secure and sustainable IoT critical infrastructure systems. Widespread adoption of policies and measures, including standardisation, training to raise awareness and codes of practice will be needed to make us all cyber literate in this next era of infrastructure development so that the world is safe, secure and resilient.

Further Reading

Ashton, Kevin. 'That 'internet of things' thing', RFID journal 22.7, 2009, 97-114.

Blackstock, Jason. Standardising a Moving Target: The Development and Evolution of IoT Security Standards. IET Conference Proceedings, 24 2018

Bonomi, Flavio, Rodolfo Milito, Jiang Zhu, and Sateesh Addepalli, 'Fog computing and its role in the internet of things', in Proceedings of the first edition of the MCC workshop on Mobile cloud computing, pp. 13-16. ACM, 2012 - available https://www.researchgate.net/profile/Rodolfo_Milito/publication/235409978_Fog_Computing_and_its_Role_in_the_Internet_of_Things/links/0deec531f19946228c000000/Fog-Computing-and-its-Role-in-the-Internet-of-Things.pdf

Boyes, H., Hallaq, B., Cunningham, J., & Watson, T, The industrial internet of things (IIoT): An analysis framework. Computers in Industry, 2018, 101, 1–12.

Bur, Jess, IoT is changing the meaning of 'critical infrastructure', Federal Times , 29 Nov. 2017 - available https://www.federaltimes.com/smr/cyber-con/2017/11/29/iot-is-changing-the-meaning-of-critical-infrastructure/

Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. 'Internet of Things (IoT): A vision, architectural elements, and future directions', Future Generation Computer Systems 29, no. 7, 2013, 1645-1660.

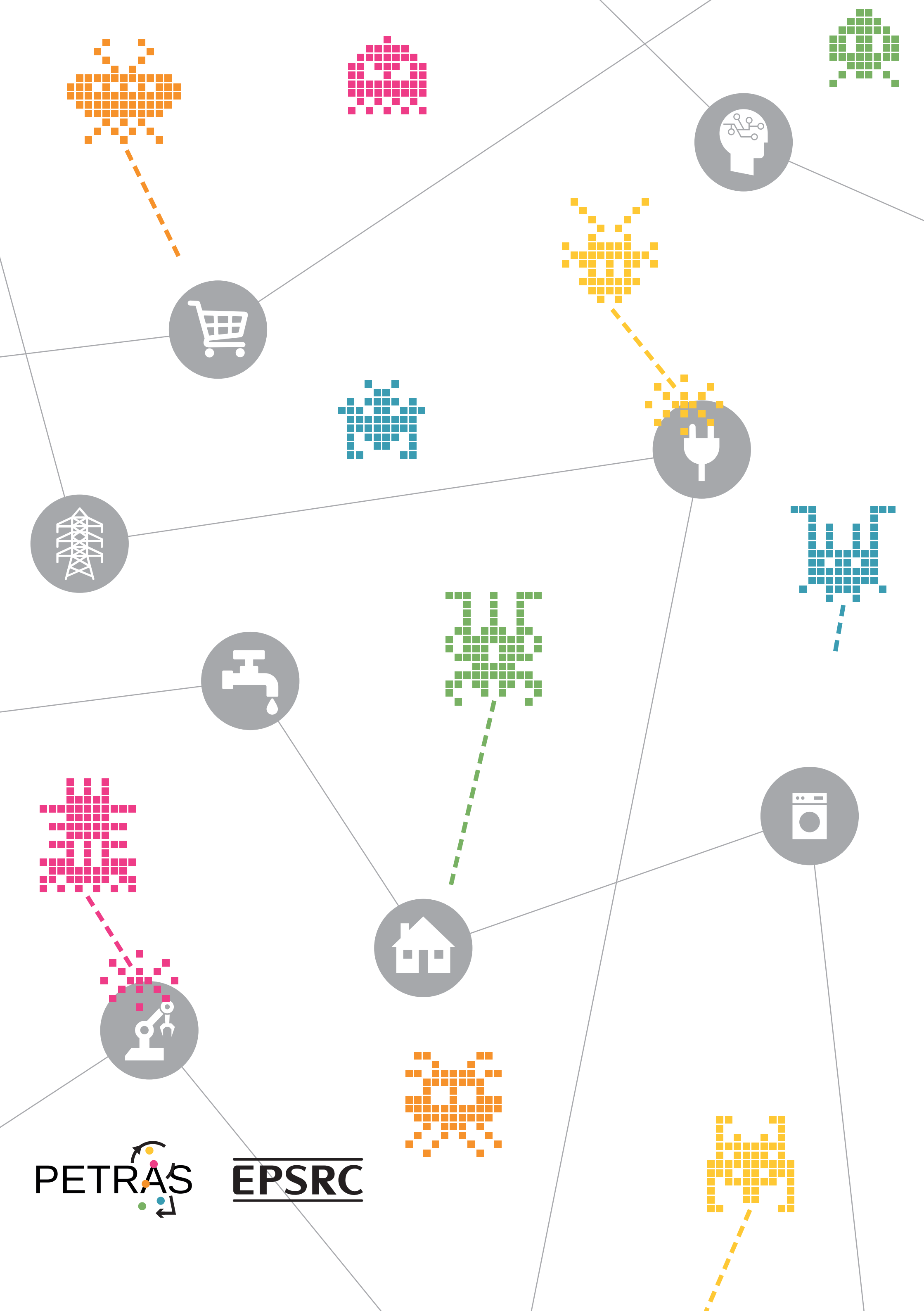
Helm, Dieter, James Wardlaw, and Ben Caldecott. Delivering a 21st century infrastructure for Britain, London: Policy Exchange, 2009.

Maggs, Colin, Great Britain's Railways: A New History, Amberley Publishing, 2018

Schwartz, Priscilla. 'Sustainable energy infrastructure: law, policy and practice', Journal of International Communications Law & Technology 4. 2009, 107.

Simon. T, Critical Infrastructure and the Internet of Things, Global Commission on Internet Governance, Global Commission on Internet Governance, 2017 - https://www.cigionline.org/sites/default/files/documents/GCIG%20no.46_0.pdf

Tanczer, L., Blythe, J., Yahya, F., Brass, I., Elsden, M., Blackstock, J., & Carr, M, DCMS Secure by Design:Literature Review of Industry Recommendations and International Developments on IoT Security. London, 2018.



PETRAS EPSRC