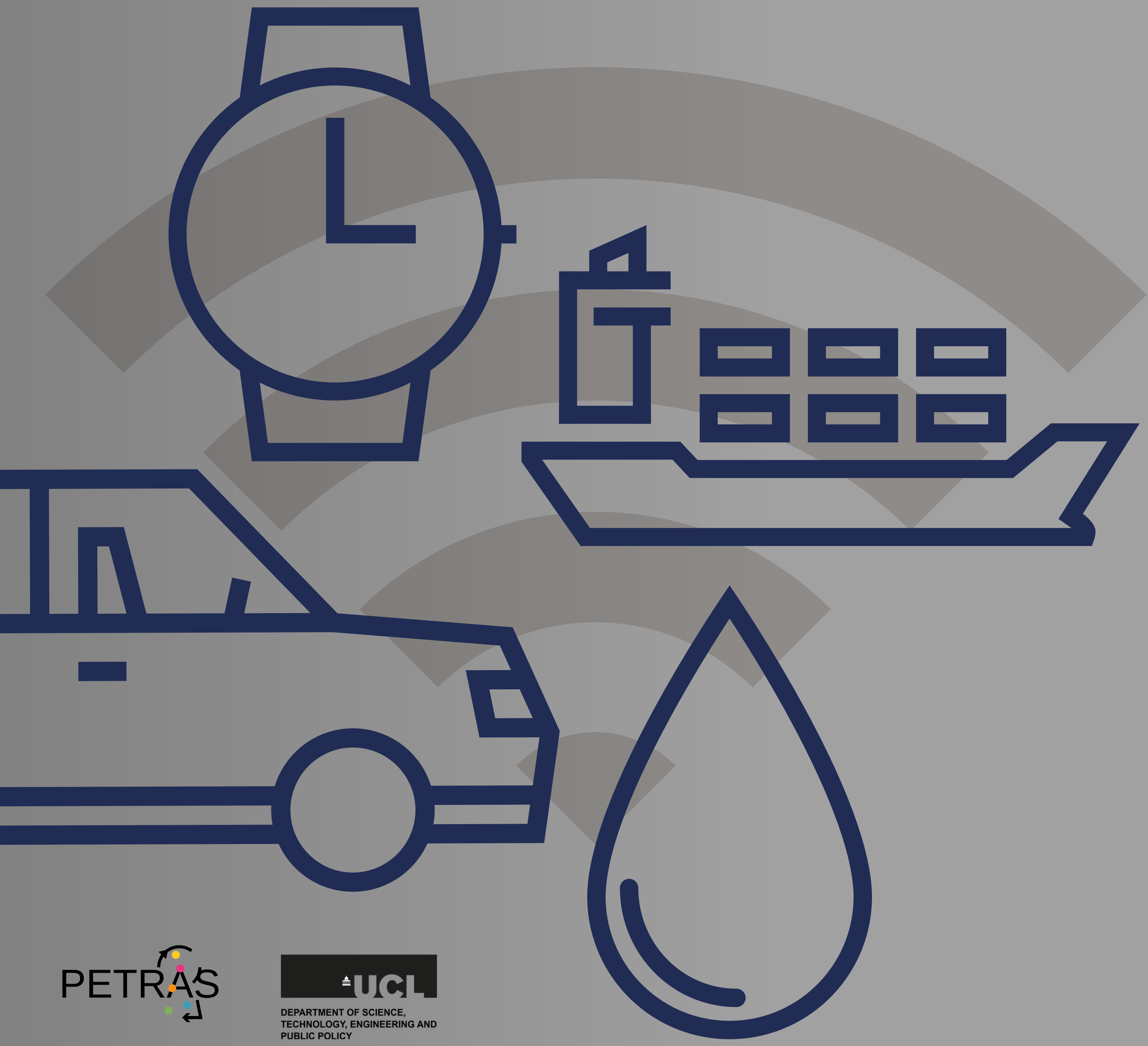
LLOYD'S

Emerging Risk Report 2018

Technology

Networked world
Risks and opportunities in the Internet of Things



PETRAS

UCL
DEPARTMENT OF SCIENCE,
TECHNOLOGY, ENGINEERING AND
PUBLIC POLICY

Lloyd’s of London disclaimer

This report has been co-produced by Lloyd's and UCL STEaPP for general information purposes only. While care has been taken in gathering the data and preparing the report Lloyd's does not make any representations or warranties as to its accuracy or completeness and expressly excludes to the maximum extent permitted by law all those that might otherwise be implied. Lloyd's accepts no responsibility or liability for any loss or damage of any nature occasioned to any person as a result of acting or refraining from acting as a result of, or in reliance on, any statement, fact, figure or expression of opinion or belief contained in this report. This report does not constitute advice of any kind.

About Lloyd’s

Lloyd's is the world's specialist insurance and reinsurance market. Under our globally trusted name, we act as the market's custodian. Backed by diverse global capital and excellent financial ratings, Lloyd's works with a global network to grow the insured world – building resilience of local communities and strengthening global economic growth.

With expertise earned over centuries, Lloyd's is the foundation of the insurance industry and the future of it. Led by expert underwriters and brokers who cover more than 200 territories, the Lloyd’s market develops the essential, complex and critical insurance needed to underwrite human progress.

UCL STEaPP disclaimer

This report, the analyses, and predictions contained herein are based on information generated through expert workshops, expert interviews, and publicly available scientific research.

While the authors of the report have taken great care in developing the analyses, readers of this report are advised that University College London’s (UCL) Department of Science, Technology, Engineering and Public Policy (STEaPP) is not engaged in the insurance, reinsurance, or related industries, and that all information provided is not intended to constitute professional advice.

UCL STEaPP specifically disclaims any and all responsibilities, obligations, and liability with respect to any decisions or advice made or given as a result of the information provided in this report. This includes all warranties, whether express or implied.

In no event shall UCL STEaPP be liable for direct, indirect, special, incidental, or consequential damages with respect to any decisions or advice made or given as a result of the contents of this information or use thereof.

About UCL STEaPP

University College London’s (UCL) Department of Science, Technology, Engineering and Public Policy (STEaPP) mobilises science, technology, engineering and policy expertise to help change the world for the better. The department hosts the Digital Policy Lab, which is a growing centre for teaching and research relevant to the pressing national and global policy challenges posed by emerging digital technologies. Members of the lab are currently working on the cybersecurity, privacy, and ethical challenges raised by the Internet of Things, international cyber (in)security, regulation and governance of the Internet, and the security of critical infrastructure.

Key contacts

Trevor Maynard, Lloyd's
Head of Innovation
trevor.maynard@lloyds.com

Madeline Carr, UCL STEaPP
Co-Director of Research
m.carr@ucl.ac.uk

For general enquiries about this report and Lloyd's work on innovation, please contact innovation@lloyds.com

About the authors

Dr Leonie Maria Tanczer is Lecturer in International Security and Emerging Technologies at UCL STEaPP. She is a former Fellow at the Alexander von Humboldt Institute for Internet and Society and a former Postdoctoral Research Associate for the PETRAS IoT Research Hub. She is researching the intersection points of technology, security, and gender and frequently runs digital security trainings.

Dr Ine Steenmans is Research Associate in 'Foresight and Futures'. She joined UCL early 2017 and her work aims to develop UCL's role as a global centre of excellence in foresight for public policy. Her work focuses on enhancing the effectiveness and efficiency by which different types of intelligence about future change are integrated into complex decision processes.

Dr Irina Brass is Lecturer in Regulation, Innovation and Public Policy and deputy lead of the MPA Programme in digital technologies and public policy at UCL STEaPP. Her research focuses on the regulation of disruptive technologies, especially digital technologies. She is working closely with policymakers and standards development communities.

Dr Madeline Carr is Associate Professor of International Relations and Cybersecurity at UCL STEaPP and director of its Digital Policy Lab. She has a strong interest in the international policy challenges posed by cybersecurity and is co-investigator for the Standards, Policy and Governance stream of the PETRAS IoT Research Hub.

Acknowledgements

UCL project team and area of expertise

- Dr Leonie Tanczer, Lecturer in International Security and Emerging Technologies
- Dr Ine Steenmans, Research Associate, Foresight and Futures
- Dr Irina Brass, Lecturer in Regulation, Innovation, and Public Policy
- Dr Madeline Carr, Associate Professor of International Relations and Cyber Security

Insurance industry interviews and consultation

- Laurence Burrows, Apollo
- Joe Mellen, Antares
- Neil Arklie, Axis Capital
- Rachael Lukehurst, Liberty Specialty Markets
- Matthew Hogg, Liberty Specialty Markets
- Rossella Bollini, Beazley
- Matt Northedge, AmTrust
- Adhiraj Maitra, Willis Towers Watson
- Ben Canagaretna, Barbican Insurance
- Kenneth Kwok, Axis Capital

Lloyd's project team

- Dr Trevor Maynard, Innovation
- Dr Keith Smith, Innovation
- Anna Bordon, Innovation
- James Burchill, Innovation
- Valentin Wittmann, Innnovation
- Craig Civil, Lloyd's Data Lab
- Linda Miller, Marketing and Communications
- Kieran Quigley, Marketing and Communications
- Flemmich Webb, Speech and Studies
- Mateo Acosta Rubio, Class of Business

Lloyd's Market Association

- Tony Elwood, Senior Executive, Underwriting
- Gary Budinger, Senior Executive, Finance and Risk

The following people were interviewed, took part in a survey and/or workshops, or commented on earlier drafts of this report; we would like to thank them all for their contributions:

Aastha Madaan, Andrey Nikishin, Anika Malde, Barnaby Craggs, Ben Hubbard, Brewster Barclay, Carsten Maple, Chris Speed, Christopher Bull, David Snelling, Feja Lesniewska, Ivana Tomic, Jason R.C. Nurse, Jan-Peter Kleinhans, John M Blythe, Karsten Schmidt, Kaitlin Haar, Marcus Chidgey, Mateusz Mikusz, Mike Hogg, Nader Sohrabi Safa, Petar Radanliev, Rafael Mantilla Montalvo, Reuben Binns, Richard Milton, Thanassis Tiropanis, as well as the remaining experts that wish to remain anonymous.

Further thanks go to the workshop participants of the Academic Centres of Excellence for Cybersecurity Research (ACE-CSR) conference for their expertise and feedback on the scenarios.

Contents

Executive summary

Overview

The Internet of Things (IoT) – devices that are connected to the Internet, collect data, and use that data to operate – is about to transform society. Everything from smart fridges and lightbulbs to remote sensors and cities will collect data that can be analysed and used to provide a wealth of bespoke products and services.

The impacts will be huge - by 2020, some 25 billion devices will be connected to the Internet (Nordrum, 2016) with some studies estimating this number will rise to 125 billion in 2030 (IHS Markit, 2017). These will include many things that have never been connected to the Internet before.

Like all new technologies, IoT offers substantial new opportunities but these have to be considered in parallel with the new risks that come with it. To make sense of this new world, Lloyd's worked with University College London's (UCL) Department of Science, Technology, Engineering and Public Policy (STEaPP) and the PETRAS IoT Research Hub to publish this report.

This study starts with the analysis of IoT's opportunities, risks and regulatory landscape. It then looks at the IoT risks for insurers in four different sectors - marine, smart homes, water infrastructure and agriculture – using ten scenarios.

Each scenario describes how IoT technology could generate and exacerbate risks that could cause losses in several lines of business.

The last section of the report focuses on IoT's implications for the insurance sector from an operational and product development perspective.

Key findings

This research presents five key findings

1. IoT will lead to data capture and management at an unprecedented scale. While this could mean better risk assessment and flexible, bespoke and real-time products; but it may also increase policyholder concerns about the use and accuracy of their data.
2. New types of threats and harms will emerge, which will increase the pressure on insurers to come up with new products and services that are closely aligned to customer needs.
3. The scale and variability of the type of disruption that could occur will affect multiple sectors and lines of business. The range of security standards that currently exist and the difficulty in establishing a baseline for IoT security will make it hard for insurers to make risk assessments in the future.
4. Insurance policies will increasingly influence and manage risk behaviour. Personalisation of policies will be capable of predicting and mitigating risks based on large scale data and trends analysis.
5. There are critical blind spots in the regulation and legislation of IoT devices and their impacts. These include uncertainties surrounding attribution and liability should anything go wrong.

Technology opportunities

IoT will drive new business growth as companies embrace the new technology and the opportunities it brings. It is important for insurers to understand how clients might adopt IoT in their business operations. This report identifies 6 main opportunity areas associated with the IoT:

1. Data aggregation. Everyday objects or physical infrastructure systems are becoming the majority of data producers and consumers (Qin et al., 2016). This places IoT as one of the major driving forces for big data analytics, for which the storage and processing of data streams is crucial.
2. Risk management. IoT technology has the potential to improve risk management processes by monitoring and controlling operations; detecting and mitigating risks through sensors.
3. Automation. IoT systems can independently react to detection of potential risk and can automate operational decisions that have been historically sensitive to human error.
4. New business models. IoT also supports the development of new business models. Industry representatives are increasingly seeing the benefits of adopting IoT technologies in their organisational processes, products, and services.
5. Sustainable business. IoT may prove a useful tool in promoting more sustainable and efficient business operation. By making effective use of supplies and assets, resource scarcity such as the rise in energy and water consumption can be addressed and profound societal challenges such as pollution or businesses impact on climate change more effectively tackled.
6. Combination with the latest technology. To fully maximise IoT's opportunities, IoT devices can be coupled with other emerging technological trends such as AI, fog computing, blockchain and smart contracts, VR, and robotics to enhance the sensorial capabilities of the evolving interdependent systems.

Technology risks

Insurers should benefit from companies' need to protect themselves from new risks they may not have had to consider before. This report identifies 6 main risk areas associated with IoT technology:

1. Multidimensionality. IoT devices and services can be a target of cyber attacks, and can multiply security and privacy risks. This could lead increased demand for cyber insurance policies as businesses seek to protect themselves from increased vulnerability.
2. Harms. Overall the impacts of IoT functionalities, and their intentional or unintentional disruption, will see the emergence of new types of harms such as loss of data, loss of privacy, loss of business, loss of reputation, exploitation, and information asymmetries. The convergence of physical and digital harm (for example, breach of digital systems leading to real life consequences such as fires, bodily injuries, and system breakdowns) will have implications on how defective products, supply chain management, safety assurance processes, and cybersecurity environments are regulated and insured. From an ethical perspective, unfair customer treatment (for examples, exclusions) and barriers to market entry based on national security considerations might arise from the adoption of IoT.
3. Scale of impact. Because of the multiple connections between IoT devices and the Internet, there is a risk that systemic failure could occur if security is breached at any one of the connection points.
4. Traditional risk assessment. As a consequence of changes in the nature of threats, losses, and vulnerabilities, the IoT will require new processes and mechanisms for risk assessments. Whereas previous cyber risk exposures were mostly limited to digital infrastructures, IoT - due to its cyber-physical nature - can have both digital and physical implications. This interplay requires risk assessments to account for both physical safety and information security, with pre-existing risk assessments having neither adjusted to this variability and scale, nor accounted for the dynamism of interconnected IoT systems.
5. Risk management. As mentioned, risk management processes could be improved by using IoT, but best practice are still being developed. Particular challenges include systemic vulnerabilities and the convergence of safety and security which do not necessarily have the same focus and are sometimes mutually exclusive.
6. Liability and attribution. With the number of stakeholders involved in IoT development and use, including manufacturers, software developers, and network and cloud providers, assigning liability when things go wrong is complex. Is a disruptive event the fault of a person (insider threat) or an actor

(criminals/terrorists), or a technical fault (e.g. algorithmic bias) within the larger IoT system? Due to the global nature of the supply chain and the diversity of IoT devices and components, the attribution of disruptive events will not only become more difficult, but also more important.

Scenarios

To illustrate the emerging changes to the nature of risks that the insurance market will face, the report includes 10 scenarios across four demonstrative sectors (critical water infrastructure, agriculture, marine, and the smart home) to unpack different risk trajectories.

The scenarios are set up to help the insurance sector explore IoT's likely impacts and are aimed at helping the industry prepare for IoT application and changes.

From an insurance perspective all scenarios show how multiple classes of insurance will be affected as different types of threat and losses become more closely connected.

IoT and insurance

IoT will also affect the insurance sector, changing how it does business and exposing it to new risks and opportunities. The report identifies five main areas that could be affected and where there is potential for new solutions:

1. New business models and customer relationships. IoT will enable insurers to personalise policies and offers. It could automate decision making and improve the pricing of risks in a range of sectors. “As-you-use" insurance policies, for example, are growing in popularity in the car insurance sector thanks to telematics, an IoT technology.

   On the commercial side, insurers could get access to the IoT data that clients collect from their sensors and devices, particularly around predictive maintenance, smart buildings, and asset tracking, such as vehicle fleets or cargo. This would help insurers create prices and polices based on the real-world performance and tailored to individual customer needs, thereby deepening customer relationships.

2. Underwriting and product development. IoT has the potential to fundamentally change insurers' underwriting and pricing models (Scardovi, 2017). By exploiting the exponential growth in data generated by IoT, insurers could know more about their customers and assets than ever before.

   This should prompt insurers to act responsibly and ethically in regards to the data and information that they hold and how they use it. IoT-generated data also allows enables insurers to respond to risks dynamically, mitigating risks, and thereby preventing or reducing claims losses. (Scardovi, 2017). IoT could further initiate product development, especially in the areas of cybersecurity and data protection. In regards to pricing models, the data provided by the IoT will enable bespoke, real-time and flexible pricing.

3. Claims. IoT is likely to drive further evolution in claims, as the sector begins to focus more on actively preventing or reducing losses. This will be driven by advances in safety technologies which will reduce accidents and, thus, premiums (A.T. Kearney, 2014).

   For example, IoT wearables and sensors placed in high-risk industries factories floors might improve safety standards, minimise risks and support compliance with safety policies resulting in lower claims for employer's liability insurance.

4. Capital reserving. Capital reserving and exposure management will be affected by IoT risks, with capital reserving potentially becoming more fluid and taking place in real-time.

   On the other hand, insurers will have to be prepared to hold enough reserves to deal with the systemic risks that IoT will generate and change capital and internal models accordingly. The challenge will be to understand and model IoT risk exposure and aggregation.

5. Modelling and exposure management. IoT will have a profound impact on risk modelling. By combining different data sets, including historical as well as real-time IoT data, insurers will be able enhance their modelling capabilities. This will be important, as IoT – more so than traditional cybersecurity risks – has the potential to aggregate risk.

   As IoT risks and opportunities emerge, more sophisticated and nuanced cyber models may need to be developed, which take account of direct and incidental cyber risks as well as operational risks caused by the use of emerging technologies. This modelling should not take place in silos, but should include dependencies and correlations that IoT risks create across different sectors.

The role of insurers in the IoT sector

Market forces alone are unlikely to drive significant changes to the IoT sector so insurers could play an important role in shaping the IoT landscape. They could:

1. Lead on data standardisation. Lloyd’s is already playing a powerful role in the standardisation of data, with data capture and integration having already been carried out as part of the London Market Group’s Target Operating Model (LM TOM, 2018a, 2018b).
2. The standardisation of data will be central to effective data capture and large-scale data analysis. Lloyd’s has the power to drive baseline requirements on which data is collected, and how it is handled and shared. This could fundamentally improve the whole insurance market, making risk modelling and product offerings more competitive.
3. Provide an environment in which the new concepts, ideas, and products that IoT data could help generate can be tested. The Lloyd’s Lab will central to this, liaising between different stakeholders to assess their needs and interpret them through innovative applications for the Lloyd’s market.
4. Proactively talk to insureds and potential clients to review and assess all risks rather than just the insurable risks associated with IoT. By taking leadership role in this space, insurers will acquire the knowledge needed to provide insureds with guidance on IoT best practice, thereby shaping the development of the IoT ecosystem in which they operate.
5. Develop scenarios and models to illustrate and quantify emerging changes to the nature of IoT. These tools would help the sector explore IoT’s likely impacts and would help the industry prepare for them. Counterfactual analysis of near-total loss events could lead to a reassessment of consequential event probabilities.
6. Work with governments, regulators and technology companies to make IoT more secure. This can result in the reshaping of business models, the opening up of new markets by these new drivers of innovation to create a useful and positive technological transformation throughout all levels of society.

Introduction

1. Introduction

Box 1: What is the IoT?

The Internet of Things (IoT) is widely regarded as a step change in the evolution of digital technologies. Although often referred to in terms of consumer devices like “smart” fridges, kettles, perhaps even cars, the IoT is not a stand-alone technology. One cannot speak of the IoT as “a thing”, but rather many different “things” connected by a network. In fact, the IoT involves a vast array of application areas that extend well beyond the home and into critical infrastructure and global trade.

The emerging IoT ecosystem is characterised by three elements (see: Tanczer et al., forthcoming):

- a proliferation of visible and hidden sensors that collect and transmit data;
- systems that interpret and make use of the aggregated information; and,
- actuators that on the basis of this information take action (often in the physical world) without direct human intervention.

These sensors can be on people (e.g. wearables or implants), on objects (e.g. cargo containers) and on physical location (e.g. warehouses) tracking all sorts of metrics including speed, level of braking, and temperature. Other geographical information systems (GIS) can also be part of the IoT network.

Innovation in the IoT is expected to lead to improvements for quality of life, for the advancement of productivity levels, and for the performance of systems such as agriculture, energy management, manufacturing, and health care.

The IoT is distinct from previous developments in digital technologies for a number of reasons.

1. The sheer scale of the IoT: by 2020, some 25 billion devices will be connected to the Internet (Nordrum, 2016) with studies estimating that this number will rise to 125 billion in 2030 (IHS Markit, 2017). These will include many things that have never been connected before.
2. The difficulties in securing very simple, but connected devices like sensors can lead to a vastly expanded cyber-attack vector with many weakened access points to critical systems.
3. In the real world, physical effects that the IoT can have blur the lines between security and safety – including in life-critical situations such as autonomous vehicles and health devices.
4. The complex global supply chains and aggregated data flows involved in the IoT complicate the definition of responsibility and liability.

All these factors will have profound effects. The data streams generated by this interconnectivity will support, amongst others, a more sophisticated risk and pricing modelling.

At the same time, the new vulnerabilities and complexities of the IoT will introduce a number of novel challenges to understanding, assessing, and managing risk. The scale and scope of change is so significant that the IoT is being described as the “Fourth Industrial Revolution” (Industrie 4.0 Working Group, 2013).

In this early phase of IoT implementation, it has already become clear that these innovations will prove disruptive on a number of levels. They will transform private and family life, reshape cities, be fundamental in critical infrastructure management, and are already introducing real change to transport systems.

In order to explore the emerging IoT risk and opportunity landscape, Lloyd's worked with University College London's (UCL) Department of Science, Technology, Engineering and Public Policy (STEaPP) and the PETRAS IoT Research Hub to identify emerging risk trajectories and opportunities for the insurance industry arising from the IoT.

Box 2: PETRAS IoT Research Hub

The PETRAS IoT Research Hub is a consortium of nine leading UK universities which work together over three years (until 2019) to explore critical issues in privacy, ethics, trust, reliability, acceptability, and security of the IoT.

The Hub was funded by a £9.8 million grant from the Engineering and Physical Sciences Research Council (EPSRC) and was boosted by partner contributions to approximately £23 million in total. PETRAS has set out to make the UK not only a global leader in the IoT realm, but also to ensure that the technical, ethical, and social issues of these systems are thoroughly explored.

Run in collaboration with IoT UK, the consortium has so far worked closely with the UK government to help develop IoT "Secure by Design" principles (Department for Digital, Culture, Media and Sport, 2018; Tanczer, Blythe, et al., 2018) and has also studied crucial issues such as "child proofing" the IoT for kids (IoTUK, 2018), worked on ethical frameworks to ensure privacy for IoT users (Mittelstadt, 2017), and provided guidance for victims of IoT-facilitated tech-abuse (Tanczer, Patel, Parkin, & Danezis, 2018b).

This study also includes the investigation of emerging risks in the IoT through four different IoT relevant sectors:

1. Infrastructure and Water

2. Agriculture

3. Marine

4. Smart Home

These scenarios help to better understand how sectors of interest to the Lloyd's market might perform under different future states. They demonstrate the changing nature of risk that a society increasingly reliant on the IoT ecosystem will face. Finally, this study offers insights into the implications of the risks emerging from the IoT for the insurance sector and its entire value chain.

For the insurance sector, IoT will offer much more effective and sophisticated ways to assess and evaluate risks. For example, in the transport sector IoT devices capture vehicular and traffic data, which in post-event liability analysis will yield a higher evidence base to use in claims and subsequent risk analysis – possibly analogous to the impact the "black box" had on the aviation incident analysis and insurance models (Lloyd's, 2017b).

Contrary to these positive outcomes, the IoT may also introduce potential for large scale, systemic failures. These could redefine losses in such a way as to require innovative thinking from the insurance sector. As reliance on the IoT increases, the safety and security vulnerabilities inherent in it will present new opportunities for malicious or accidental exploitation. The possible consequences of such actions raise compelling questions about the future of risk management.

1.1 Regulatory frameworks and IoT security baseline

A key challenge to managing new risks introduced by the IoT is that existing policies and regulatory frameworks are currently not providing sufficient incentives and corrective measures to ensure that all entities in the IoT supply chain internalise the cost of security into their businesses.

This has led industry consortia, standardisation organisations, regulators and policy-makers to consider the development of a baseline of IoT security (Brass, Tanczer, Carr, Elsden, & Blackstock, 2018).

These developments are particularly relevant for brokers and insurers who will want to refer to best practices in their risk assessment and underwriting decisions where IoT is deployed.

Establishing a baseline for IoT security is proving a difficult task for several reasons:

- Diversity of IoT application domains, from consumer goods, to transport, to utilities and industrial systems.
- Variability of IoT system topologies across these application domains, from IoT in the home (which might have a centralised topology), to IoT in critical infrastructure (which will require integration with existing control systems and operational technologies).
- Increasingly blurred boundaries and interdependencies between data integrity, cybersecurity, physical security, safety, reliability, resilience, and service availability.
- Balance between overarching horizontal security specifications and vertical industry requirements.
- Lack of motivation to pay for security features which may need regulation to overcome the scarce market force incentives (Bauer, Burkacky, & Knochenhauer, 2017).

The difficulties of setting a baseline for IoT security also complicate current legislative initiatives to promote certification schemes for IoT security, both in the United States and in the European Union (EU). However, in the absence of clear and comprehensive standards for IoT security, such schemes could become obsolete very quickly – especially given the fast pace of cybersecurity threats that emerge in and from the IoT.

Thus, in order to develop clear and comprehensive standards for IoT security and safety, the increased connectivity of physical objects and infrastructures requires better alignment of regulatory frameworks for safety, security, data protection, and liability. Such standards will then facilitate proactive responses to the new cyber-physical risks that the IoT introduces (See Box 3).

Box 3: IoT security and relevant regulatory frameworks in the EU

At the moment, in the EU, there are four main regulatory frameworks that apply to aspects of IoT security.

With regard to cybersecurity, the Network and Information Systems (NIS) Directive 2016/1148 specifies legal standards for digital service providers and operators of essential services in critical sectors such as energy, water management, transport, financial market infrastructures, as well core digital infrastructures. The Directive covers security requirements, incident handling, business continuity management, monitoring, auditing, and testing.

It also stipulates the identification of a competent national NIS authority in each EU Member State; the establishment of a cooperation mechanism for cybersecurity incident response; and information sharing of cybersecurity risks associated with the operation of essential services in national critical infrastructures. The NIS Directive was transposed into national legislation in May 2018. As the first legislative measure on cybersecurity in the EU, the NIS Directive has paved the way for a regulatory proposal that would establish the European Union Agency for Network and Information Security (ENISA) as the Cybersecurity Agency of the EU. It has similarly prompted the production of an initially voluntary cybersecurity certification scheme, aimed at harmonising the procedures and instruments for testing and showing conformity with a responsible level of cybersecurity.

With regard to safety and the reliability of cyber-physical systems, such as automotive vehicles, there are currently several proposals in the EU to broaden current product safety legislation (e.g., Directive 2001/95/EC) to reflect new cybersecurity, data integrity, and product safety concerns. If successful, these proposals will modify current safety regulations in the EU in a manner that would make cybersecurity a component of the overall safety of products and systems. If these regulatory changes are successful, will they make current cybersecurity certification proposals redundant, or will they require further integration of safety and security regulations, with type approval and certification schemes?

These proposals will also have direct implications on current liability frameworks for defective products, as stipulated in EU Directive 85/374/EEC. The European Commission (EC) has recognised the challenges of embedding digital technologies in physical products and systems. It recently proposed a revision of the directive, in order to evaluate whether its definition of a “product defect” (Art 6) captures “products where software and applications from different sources can be installed after purchase, products performing automated tasks based on algorithms, data analytics […] or products purchased as a bundle with related services”.

Another major regulatory framework that applies to IoT security is the General Data Protection Regulation 2016/679 (GDPR). While the GDPR is directly concerned with the responsible processing of personal data, and establishing rules relating to the free movement of personal data, it also introduces obligations with relevance to IoT security. The GDPR establishes the principle of “data protection by design and by default” (Art 25) and stipulates that data controllers carry out a data protection impact assessment “where a type of processing in particular using new technologies […] is likely to result in a high risk to the rights and freedoms of natural persons” (Art 35).

In this case, are we witnessing a blurring of boundaries between the protection of personal data, the integrity of the data, and the integrity of the entire cyber-physical system that allows data to be captured and exchanged in a secure manner? This is of fundamental importance to digital forensics and insurers, who have to rely on the integrity of the data in order to verify claims and design tailored policies for their customers.

While these frameworks demonstrate the increased awareness by regulators and legislators to the emerging risks posed by digital technologies such as the IoT, it also reveals the complicated task of integrating all aspects of IoT security and safety into comprehensive standards and regulations.

In addition, given that IoT supply chains are global, such measures raise concerns about their effectiveness outside their parent jurisdictional boundaries and their potential rigidity to the rapidly changing nature of vulnerabilities and risks that IoT brings.

In response to some of these concerns, several industries are developing their own technical specifications, guidelines, and self-regulatory frameworks to establish a baseline of IoT security, such as:

- The Open Connectivity Foundation for the security of smart white goods.
- The Industrial Internet Consortium for the security of manufacturing, health, and industrial IoT.
- The Cybersecurity Charter of Trust in Aviation (See Box 4).

Overall, it is evident that the regulatory landscape for managing IoT risks is changing at a very fast pace. The insurance sector has to prepare not only for proposals established in key jurisdictions such as the EU and the United States, but also for the emergence of self-regulatory frameworks developed by industry alliances and consortia.

The market is directly affected by these transformations and faces choices in whether to refer to IoT security and safety guidelines in their policy design, as well as promote best practice in key industry sectors where IoT risks are beginning to take form, including transport, utilities, and industrial processes.

Box 4: The Cybersecurity Charter of Trust: successfully integrating IoT security in the aviation supply chain?

Led by Siemens, the Charter of Trust is an industry-led agreement established to promote responsible cybersecurity practices in connected aviation. The Charter is designed to establish three primary goals:

1. To protect the data of individuals and businesses;
2. To prevent harm to people, businesses, and infrastructure;
3. To establish a reliable basis where confidence in a networked, digital world can take root and grow.

The Charter is a good example of a vertical industry alliance that is promoting an integrated approach to IoT security – spanning across design and business practice. The Aviation Charter of Trust was designed to engage the entire supply chain for connected aviation, from aircraft manufacturers such as Airbus, to hardware providers such as Siemens, including insurance providers.

1.2 IoT and insurance

While current IoT devices may appear simple and are, at this early stage, frequently lacking interoperability with other systems, market forces are rapidly broadening the competencies of devices while developing new ones.

This process goes hand in hand with the growth of artificial intelligence (AI), machine learning and the emergence of blockchain technologies. Together, these developments should enable future IoT devices to independently act and make decisions based on collected data and seamlessly aggregated information.

The anticipated rise of IoT in many sectors ranging from agriculture to utilities management, suggests that the insurance sector itself may benefit from picking up these new devices and techniques (i.e., data analytics, machine learning) to address new customer demands in a fast-moving and technology-driven environment (Braun & Schreiber, 2017).

Additionally, IoT applications such as wearables or industrial appliances have the potential to passively monitor the state and wellbeing of both individuals and infrastructures and provide continuous risk information for more accurate risks assessment.

We believe IoT will have an impact on the entire insurance value chain ranging across underwriting, claims, and modelling activities. We expect IoT to enable the insurance sector to support business decision making and to improve pricing and capital calculation. IoT will generate new business models due to the influx of directly available, unfiltered, and granular data streams. In particular, IoT's interconnection with AI (see Section 2) and AI's current uncertain legal status[a] are further opening up insurable markets.

InsurTech

InsurTech refers to the employment of technological systems like the IoT to improve efficiency in the insurance sector, including in risk detection and prevention (Puertas et al., 2017). To date, InsurTech comprises technology start-ups which are challenging the previous distribution model of the insurance sector, offering insurance interface, tailored solutions, and on-demand products (Puertas et al., 2017).

The rapid growth of InsurTech is catching up with the banking-focused FinTech sector (PwC, 2017a): in the first half of 2017, Accenture and CB Insights estimated that £218 million was invested into InsurTech businesses in the UK (Williams-Grut, 2017), with the global investment in InsurTech having surged by 247% to $985 million in the second quarter of 2017 (PwC, 2017c).

While a lot of the work in InsurTech has focused on developing more efficient and cost-effective ways of transacting personal and small commercial lines, these innovations also have real implications for corporate risk managers (Banham, 2017).

The technological changes are expected to lead to cross-cutting amendments of insurance offers and practices, such as simplification of policy management, reduction of "moral hazard", and lowering the costs of payments by having a consent stream of real-time data (see Section 5 for a more in-depth discussion on IoT's effects on the insurance market).

InsurTech provides a good example of the opportunities and risks that IoT brings. On the one hand, the increased embeddedness of IoT technologies in existing products and infrastructures offer great opportunities for insurers to understand policyholders' needs and to provide more tailored services that protect their customers against known risks, such as natural disasters.

On the other hand, the increased embeddedness of IoT exposes new types of risks, pertaining to cybersecurity, the cyber-physical reliability of an infrastructure or a process, and the integrity of the data that provides valuable forensic information when verifying insurance claims or apportioning liability.

[a] There are ongoing discussions about algorithms ability to have legal personality and be held liable (see: Select Committee on Artificial Intelligence, 2018).

A changing opportunity landscape

Emerging Risk Report 2018

Technology

2. A changing opportunity landscape

The IoT has been recognised as one of the technological advancements at the centre of the Fourth Industrial Revolution. According to Klaus Schwab, Founder and Executive Chairman of the World Economic Forum (WEF), we are currently entering a new industrial era driven by the increased interconnectedness of new physical, digital, and biological technologies (Schwab, 2016).

Thus, we are witnessing a shift in the value add of digital technologies from connecting people and organisations to connecting machines, devices, people, organisations, physical infrastructures, and services.

Governments around the world are beginning to consider the direct and indirect effects of the IoT on their economy and public services. For instance, in 2014, the UK government published the Blackett Review (UK Government Chief Scientific Adviser, 2014), which highlighted the social and economic potential of the IoT. The review identified five strategic sectors that could bring socio-economic benefits from the application of IoT in transport, energy, healthcare, agriculture, and the built environment.

Since then, the UK government has recognised the IoT as a driver of socio-economic innovation and growth in its Digital and Industrial Strategies, and has invested considerably in research, demonstrators, and test beds for smart cities, critical infrastructure, transport, and health. Similar strategies have been adopted by other governments across the world, including Singapore[b], China[c], Brazil[d], Australia[e] and the United States[f].

Using the number of machine to machine (M2M) connections as a proxy for IoT investment, a latest report published by Frontier Economics (2018) shows a 10% increase in M2M connections would generate an increase in GDP of $370bn in Germany and $2.26trn in the US over the next 15 years (2018-2032).

[b] Singapore is at the forefront of smart city progress. It not only active in developing smart building constructions and smart grid implementation, but also finances the development of new technologies and has implemented projects related to the digitisation of cultural and tourism facilities (PwC, 2017b).

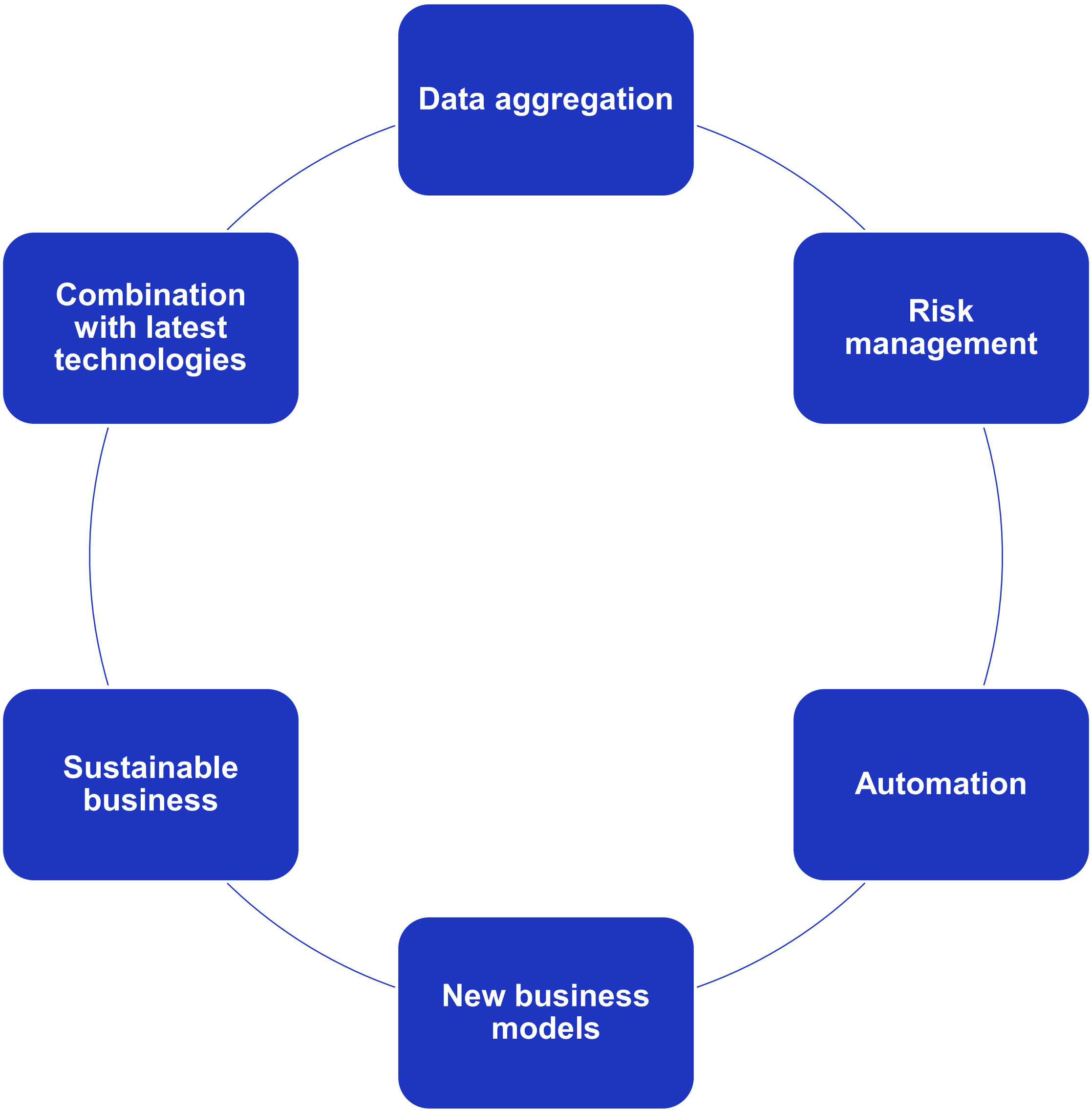
[c] In 2015, China introduced its ‘Internet Plus’ strategy which was an attempt by Chinese policymakers to boost the Chinese economy. In particular, IoT was considered a major driving force with initiatives focusing on funding for research and development, as well as a heightened broadband connectivity (Hristov, 2017).

[d] In 2017, the Brazilian government launched a national strategy for the deployment of IoT technologies. The four core verticals of the strategy focus on smart cities, healthcare, agriculture, and manufacturing (Brazilian Development Bank, Ministry of Planning, Budget, and Management, & Ministry of Science, Technology, Innovation and Communication, 2017).

[e] For instance, the IoT Alliance Australia is a national industry body that has as its purpose the activation and support of collaboration across industry, government, research, and communities, and to drive evidence-based input into appropriate IoT policy and regulation.

[f] The United States has already put forward legislation (i.e., IoT Cybersecurity Improvement Act 2017) seeking to address IoT vulnerabilities (Senate of the United Staates, 2017). It provides minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes.

Figure 1: The opportunities landscape



Source: Lloyd's – UCL, 2018

2.1 Data aggregation

A core opportunity that the emerging IoT environment brings is the ability of enhanced data aggregation. Everyday objects or physical infrastructure systems are becoming the majority of data producers and consumers.

This is a shift away from an environment in which data producers and consumers were primarily human beings (Qin et al., 2016). This places IoT as one of the major driving forces for big data analytics, for which the storage and processing of data streams is crucial.

The efficient processing of these data streams will benefit from further innovation enhancing data interoperability and completeness.

– Reducing status uncertainty. Data collection sensors can provide higher precision and frequent information about the location and status of assets. This not only allows for monitoring a system in real time and adjusting its operational conditions accordingly, it also means that in the immediate aftermath of a major disruptive event, it will be possible to capture a snapshot of the likely scale of impact.

2.2 Risk management

Risk management processes can be improved through IoT technologies. As risk management begins with threats and vulnerabilities, access to larger datasets generated by IoT devices can help to understand more clearly how likely threats are to occur.

While the report at a later stage *(see: Section 3)* highlights some limitations that IoT brings to traditional risk assessment models, there are advantages and enhancement opportunities, including:

– Monitoring risk. The status, operation, and environment of a connected system can be comprehensively monitored through sensors. Alerts can be sent when changes to the system occur, operational behaviours are altered, or goods do not follow a pre-approved route.

  The monitoring functionality offered by IoT systems is extremely valuable for high-risk sectors, including in medical settings.

– Controlling risk. The monitoring function has as a consequence that owners and operators of IoT system have controlling oversight over goods, including the physical hardware, a product's software and the data deriving from it.

  In particular the remote-control functionality ensures that amendments can be implemented from afar and is helpful for sectors where goods are in constant movement, including the maritime, aviation, and general manufacturing space.

– Detecting risk. The monitoring and controlling function of IoT also ensures that potential upcoming errors or faults can be proactively spotted by the system. Sensors can measure and assess the system and through the comparison with average "normal" level identify if anomalies could occur.

  This is useful in instances where products are in constant and longitudinal usage, including the erosion of pipes or the abrasion of machinery.

2.3 Automation

As previously introduced, IoT systems can independently react to detection of potential risk – a key feature for the IoT-supported enhancement of automation. Examples include the automation of the so-called "connected" or "smart" home, the automation of transport systems through connected and increasingly autonomous vehicles, as well as the automation of industrial environments, including power plants, robots, or general control systems.

– Reducing human error. Digitally-connected actuators can automate operational decisions that have been historically sensitive to human error. Automation can thereby serve as an aide to human performance and decrease the level or workload and level of difficulty to manage particular tasks (Wickens & Dixon, 2007).

2.4 New business models

IoT also supports the development of new business models. Industry representatives are increasingly seeing the benefits of adopting IoT technologies in their organisational processes, products, and services, with IoT becoming a new platform for E-business (Zhang & Wen, 2017).

The latest IoT Barometer noted that the rate of adoption has more than doubled in five years, from 12% in 2013 to 29% in 2017, with transport and logistics and retail seeing the largest year-on-year growth (Vodafone, Analysys Mason, & Circle Research, 2017).

Early business adopters are also becoming more sophisticated with their integration and use of IoT in their business processes, with 46% of surveyed companies integrating IoT in core systems such as enterprise resource planning.

– Increasing efficiency and reducing costs. An example to highlight IoT's ability to increase operational efficiency can be seen in the healthcare sector, where ambulance services in New Zealand are using real-time updates on the availability and location of ambulances to link these to the existing capacity of nearby hospitals (Vodafone et al., 2017).

  IoT and the use of big data analytics will also create "greater flexibility in the scale and scope of production". This is seen in the agriculture sector, where farmers can manage yield through a combination of soil, weather, and machine sensors.

Box 5: Harnessing IoT data through cloud computing

Cloud computing has virtually unlimited capabilities in terms of storage and processing power. As these are the main drawbacks of IoT, linking cloud computing with IoT could bypass such constraints (Díaz, Martín, & Rubio, 2016). Many businesses such as the technology company Philips and power company Enel are already using cloud computing platforms such as the Amazon Web Service (AWS) to make effective use of IoT-generated data.

Technology-focused health insurance companies are now starting to connect these elements with IoT applications for their customers. The latter receive wearable devices to track each their health and fitness status through a mobile app that includes step tracking, a doctor finder, access to health history, and the doctor on call feature.

2.5 Sustainable business

IoT may prove a useful tool in promoting more sustainable and efficient business operations. By making effective use of supplies and assets, resource scarcity such as the rise in energy and water consumption can be addressed and profound societal challenges such as pollution or businesses impact on climate change more effectively tackled.

While e-waste resulting from IoT is an issue that requires far more examination, developments to use ecologically sustainable materials and to both implement and practice a circular economy can keep resource usage to a minimum.

For example, "Green IoT" embodies the idea to apply energy efficient procedures in both hard- and software and to make the entire life cycle of IoT (i.e., design, production, utilisation, and disposal) more environmentally friendly. It is targeted at facilitating a reduction of the greenhouse effect and can reduce the greenhouse footprint of an individual business (Shaikh, Zeadally, & Exposito, 2017).

There is scope to promote this approach on a larger scale, with bodies such as the Institute of Electrical and Electronics Engineers (IEEE) Communication Society having established a technical subcommittee that hopes to enhance and ultimately develop standardised energy-efficient communications and computing solutions (Shaikh et al., 2017).

Combination with the latest technologies

To fully maximise IoT's opportunities, IoT devices can be coupled with other emerging technological trends that enhance the sensorial capabilities of the evolving interdependent systems:

- Machine learning (ML) and artificial intelligence (AI). When IoT is coupled with ML applications and in the future fully operational AI, IoT's "smartness" and ability to identify, learn and act upon pattern is made possible (Assem, Xu, Buda, & O'Sullivan, 2016).
- 5G. The fifth generation of mobile networks will ensure a much faster communication transfer, much lower latency and far greater capacity to deal with the technological advancement that IoT will both create as well as require.
- Fog computing. Fog computing – which is a new paradigm for distributed computing and sometimes referred to as "edge computing" – is a technology that aims to bridge the gap between remote data centres and IoT devices by analysing time-sensitive data at the network edge, close to where it is generated instead of sending vast amounts of IoT data to the cloud (Alrawais, Alhothaily, Hu, & Cheng, 2017; CISCO, 2015).
- Blockchain and smart contracts. Blockchain as a technology which uses public-key cryptography to create "a tamper-proof" digital ledger of transactions which is then stored and recorded on a distributed ledger. It is considered as a potential means to, for instance, automate business transactions between smart devices (Kshetri, 2017). This ability to facilitate monetary transaction is enabled by "smart contracts" that enforce obligations between the two exchanging parties.
- Virtual reality, augmented reality, and mixed reality (The new realities: VR, AR, MR). While VR is a means to create a "virtual" and, thus, completely "new" world, AR will "augment" and transform the reality that exists on top of the "real" world and MR allow to entwine both together. In all of these three contexts, IoT sensors could help to make the lived experience as well as these system's functionalities more comprehensive (Deloitte, 2017). See our report 'New realties: risks in the virtual world' for more information in this area. '
- Advanced robotics. This can include service robotics (SRI Consulting Business Intelligence, 2008) as well as co-robots that are intended to physically interact with humans in a shared workspace and will profit from the sensorial data generated by IoT devices.

- Encryption. To ensure their security of generated data, and overarching infrastructure such as the communication network, IoT systems need to maintain strong encryption.

  An emerging concern is the future challenge posed by fully operational quantum computers that will have orders of magnitude enhanced capability in probing advanced encryption systems.

  Recent research in the field of postquantum cryptography, however, is developing cryptographic algorithms potentially capable of withstanding such attacks (Buchmann, Lauter, & Mosca, 2017).

Box 6: IoT and blockchain

A recent study by Gatteschi et al. (2018) analyses several blockchain use cases taken from the insurance sector. The authors consider the insurance industry a space that has the full potential of this technology not yet explored.

The research team offer a Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis to identify the advantages and disadvantages of the adoption of blockchain by the sector. Their study indicates that blockchain could be deployed, for instance, to operationalise smart contracts, speed up claims processing, and reduce operating costs.

While Gatteschi et al. (2018) believe that blockchain is a tremendous invention, they still see needs for several improvements before becoming mainstream in the sector. Reasons for that include:

- limitations of blockchains scalability;
- complexities in relation to its usage;
- the lack of a “winning” blockchain that will be supported over a prolonged period of time; as well as
- the absent best practice to develop “free-of-bugs” smart contracts.

A changing risk landscape

Emerging Risk Report 2018

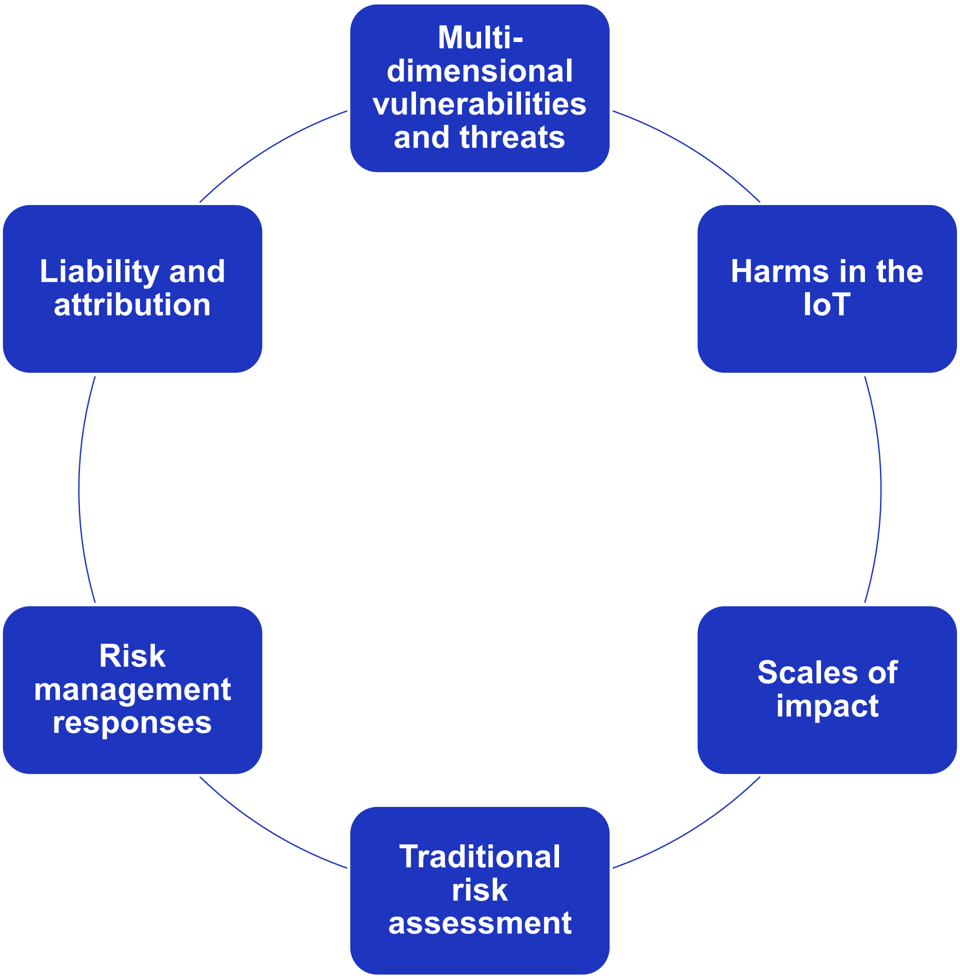
Technology

3. A changing risk landscape

As the IoT emerges and early adopters experiment and innovate, its opportunities and use cases will become more evident. However, with IoT's embeddedness of connected chips, sensors, receivers, and actuators across different sectors and within assets of vastly divergent functionalities and values, questions arise about the type of systemic challenges that may follow.

Questions also arise about the implications of the risk landscape resulting from the changing nature of error, threat, harm, vulnerability, and exposure. It is important to improve our understanding of what those changes will mean for the ways in which risk is assessed and managed, and also for the ways in which challenges of liability and attribution are resolved.

Figure 2: The risks landscape


Multi-dimensional vulnerabilities and threats
Harms in the IoT
Scales of impact
Traditional risk assessment
Risk management responses
Liability and attribution

Source: Lloyd's – UCL, 2018

3.1 Multi-dimensional vulnerabilities and threats

The IoT will introduce new vulnerabilities and threats. IoT devices and services can themselves be a target of attacks and offer pathways through which the introduction of the IoT into physical systems creates security and privacy risks (Loit, Sivanathant, Gharakheilit, Radford, & Sivaramant, 2017).

A classification system of IoT threats and their levels of criticality was recently proposed by the ENISA. ENISA (2017a) mapped out the multi-dimensional range of vulnerabilities introduced by the IoT, where vulnerabilities and threats can affect:

- Devices such as sensors, actuators, software, hardware;
- Other devices in an IoT ecosystem that interface with a target device;
- Communications networks and protocols;
- Infrastructures such as routers, gateways, power supplies;
- Platforms and back ends such as cloud services;
- Decision-making processes driven by algorithms (and the biases these may contain);
- Applications and services; and
- Information at rest, in transit or in use.

In the absence of a defined baseline for IoT security, this classification may be useful for insurers to identify the most critical points in the IoT ecosystem when designing policies. It is applicable to a range of IoT systems that have previously been proven to be vulnerable, including implanted cardiac devices, cars, or smart meters (Spring, 2016; Tanczer, Brass, Elsden, Carr, & Blackstock, forthcoming).

Legacy vulnerabilities

Internet-connected devices are understood to be vulnerable to malicious attacks or accidental failures propagated across the network. Many IoT devices are currently too small to have the computational power necessary to incorporate dynamic security features, such as software updates or patches. In addition, within a highly competitive global supply chain manufacturers often lack the incentive to absorb the costs of security into their business practices (ENISA, 2017a).

On the demand side, research by McKinsey has found a disconnect between semiconductor companies' desire for security and their willingness to pay for it (Bauer et al., 2017). On the commercial side, research by Blythe and Lefevre (2018) investigated IoT users' willingness to follow the security advice, with users most willing to perform password behaviours e.g. “not sharing passwords”; “use strong passwords” and less willing to perform network behaviours e.g. “isolate devices onto their own network”. This demonstrates that behaviours that require higher technical capability are at the personal level less likely to be adopted by consumers.

As a consequence, insecure devices increasingly penetrate global markets. Installed in diverse systems at home, the workplace or in commercial settings, IoT systems frequently lack minimum security specifications such as software updates and vulnerability disclosure policies. Once installed, vulnerable IoT devices provide a permanent gateway to the wider network that they connect to.

Exacerbating this further is the fact that many of these simple, insecure devices are expected to remain functional and in place for decades as opposed to the much shorter lifecycle of connected devices in the past.

Box 7: IoT software updates

To keep IoT systems secure, manufacturers will be expected to continuously test them against latest types of attacks, react to newly found security vulnerabilities, and diligently update the device's software. Kleinhans (2017, 2018) raises important questions about the contestation nature that remains when it comes to vendors and user's responsibility and ongoing developments on IoT security certification.

To date, no clear guidelines exist for the duration over which manufactures have to provide software updates for their products. This creates uncertainty and opens up avenues for discussions on liability and negligence. For the insurance market, the ambiguity could pose a significant risk.

IoT as attack vector

In addition to rendering assets vulnerable to failure in the ways described above, the IoT can itself be changed into an attack vector. The Mirai botnet in Box 8 is an example of the use of IoT becoming the vector for a cyber-attack.

Box 8: Mirai botnet

In 2016 the Mirai botnet turned globally dispersed IoT devices, such as video cameras and TV sets, into remotely controlled assets. These were used in one of the most powerful Distributed Denial of Service (DDoS) attack seen to date, at 1-TBps, the equivalent of streaming 1000 hours of Netflix in a second (Gallagher, 2016).

The botnet led to the take down of the Domain Name System (DNS) services provider Dyn, resulting in disruptions to the critical Internet infrastructure. Users were unable to reach Dyn's customers' sites, which included Twitter, PayPal, and Amazon.

The attack also had long-term financial repercussions for Dyn. According to Bitsight, a security rating platform, approximately 8% of Dyn's DNS customer base terminated their contract after the attack (Paul, 2017).

While the source code for Mirai primarily targeted consumer devices, the lesson here was that the equally insecure IoT-enabled infrastructure which businesses rely upon could similarly be used against asset owners and operators in the near future.

One of the crucial takeaways to be learned from Mirai, is that the DDoS attack exploited basic security vulnerabilities that are already well known to security professionals, predominantly the use of default passwords.

Since Mirai, several IoT-enabled DDoS attacks have been recorded, exploiting similar vulnerabilities in insecure consumer devices, by accessing the botnet source code online, through a simple web search.

This led security analysts at Cisco to conclude that known vulnerabilities in IoT devices and systems, coupled with the rapid growth in the number of connected IoT devices around the world, have brought about new types of attack, coined "Destruction of Service" (Brass et al., 2018; Cisco, 2017).

3.2 Harms in the IoT

The impacts of the IoT functionalities, and their intentional or unintentional disruption, will see the emergence of new types of harms:

- Loss of data. Data will increasingly become perceived as an asset vulnerable to losses.
- Loss of privacy. There are key vulnerabilities in ensuring the confidentiality of sensitive data (Apthorpe, Reisman, Sundaresan, Narayanan, & Feamster, 2017).
- Loss of business. Failure of devices can lead to disruption of data and goods transactions.
- Loss of reputation. Data breaches have been shown to negatively affect a company's reputation (Alva, 2018).
- Exploitation. New forms of power abuses can emerge, including in instances of employee surveillance or sexual and domestic violence and abuse as well as coercion and control (Tanczer, Patel, Parkin, & Danezis, 2018).
- Information asymmetries. The choice to abstain from sharing data or using certain devices may lead to adverse consequences.

Convergence of physical and digital harm

The IoT blurs the lines between the historically more distinct domains in which physical and digital harm unfold. Remote digital access to systems can now lead to real life consequences such as fires and bodily injuries. System breakdowns can have major consequences for coupled critical infrastructures in core utilities, leading to power disruptions or limiting access to other essential services.

The rapid increase in automation and connectivity of devices raises important questions about our readiness to understand and regulate interdependencies in cyber-physical systems that integrate computation, communication processes, and physical systems in smart (Brass, 2018).

These have several implications for how governments currently regulate defective products, supply chain management, safety assurance processes, and cybersecurity environments (Brass, Carr, Tanczer, Maple, & Blackstock, 2017).

- Political conflict and terrorism. A major dimension to the convergence of physical and digital harm relates to the misuse and exploitation of IoT systems by state and non-state actors for, for instance, political violence or terrorism.

The safety and security of IoT-supported critical infrastructure systems is of great importance as there may be a temptation to attack power grids or transportation infrastructures (DeNardis & Raymond, 2017).

Ethical, economic, and legal challenges

There are a number of ethical, macro-economic, and legal issues that may arise as a consequence of the large-scale deployment of emerging technologies, including:

- Access issues and exclusions. The potential to disadvantage particular groups of users in competitive insurance markets (EIOPA, 2017). For example, consumers with a higher risk profile may face access issues or exclusions as a result of enhanced risk assessments.

  Unfair treatment. The willingness of some consumers to voluntarily choose to share data gathered through IoT technologies may create unfavourable outcomes for those who do not wish to do so (Tanczer, Carr, Brass, Steenmans, & Blackstock, 2017). Such developments may be problematic with regard to the expectations of the Treating Customers Fairly (TCF) principle as they could be used to price risks that do not reflect the behaviour or choices of the individual.

- Market access. The use of national security considerations to prevent particular players from accessing domestic markets (e.g., US versus Huawei).

Thus, national security concerns may be legitimately applied to ensure the safety and security of a country, but may also open the possibility to be used as tool to foster national economic interests. IoT technologies may therefore become entangled in geopolitical trade disputes.

Box 9: Connected and autonomous vehicles (CAVs)

Although CAVs are sometimes portrayed as a ‘thing of the future’, they are very much part of the presence. The UK government has already committed £15 million to developing a ‘connected corridor’ from London to Dover (A2/M2), trialling in-vehicle, vehicle-to-vehicle (V-2-V), and vehicle-to-infrastructure (V-2-I) systems. These complex systems rely on several, interconnected IoT technologies – sensors, actuators, and operational technologies, local and cellular communication networks – that collect, record and transfer large amounts of data. In order for real-time traffic to take place in a safe manner, it is imperative that the data is exchanged securely and reliably, ensuring its protection as well as its integrity.

However, as automotive vehicles become more autonomous, connected, and able to exchange information they also become more vulnerable to attacks. In such dynamic environments, an attacker may exploit a number of minor vulnerabilities that emerge as the result of component updates by different entities, each of little significance on their own, but with damaging interactive consequences for system integrity and vehicle safety within the connected environment (Brass, 2018).Recognising these challenges, the UK government published a voluntary code of practice that establishes Key Principles of Cyber Security for Connected and Automated Vehicles (Department of Transport & Centre for the Protection of National Infrastructure, 2017) targeting the entire supply chain for automotive vehicles, including sub-contractors and service providers.

Some of the key principles propose that manufacturers have “an active programme in place to identify critical vulnerabilities and appropriate systems in place to mitigate them in a proportionate manner” (3.3), and that “they ensure their systems are able to support data forensics and the recovery of forensically robust, uniquely identifiable data” (3.4). However, meeting these recommendations require considerable operational and computational capacity, as well as reliable and secure communications (Brass, 2018).

For insurers, it will become increasingly important to identify and understand the new vulnerabilities that emerge in these complex cyber-physical systems, where data travels across several objects and infrastructures, and is exchanged in several jurisdictions. Mapping these new vulnerabilities against existing risk classifications, and identifying gaps, is an important next step.

3.3 Scales of impact

Increased data availability and interdependencies have manifested in multiple ways since the growth of the Internet. Three features of IoT systems are going to lead to a transition to significantly heightened impact of disruptive events and vulnerabilities:

- Connectedness and access. Previously independent and segregated devices are now subject to complex interdependencies in "systems of systems". The integrity and access control of devices (Liu, Xiao, & Chen, 2012) in light of this increased connectivity leads to the erosion of sector boundaries.
- Continuity. Unlike IT systems that can be temporarily taken offline in order to address security problems, IoT systems have availability as a fundamental requirement (Cam-Winget, Sadeghi, & Jin, 2016). This "always on" prerequisite means that that periodic risk assessment of IoT systems will be insufficient.
- Data integrity. Erroneous data in one system may potentially "pollute" others. The increasing reliance on the integrity of data that supports automated decision making – often in systems that aggregate multiple data flows - may heighten the potential for accidental or malicious implications of erroneous data.

These result in two changes to the risk landscape:

- Amplification – accumulative, intra-system risk. Access to one IoT device frequently enables access to other IoT devices in the same environment (e.g., the "smart" home; UL, 2017).
- Cascading – correlating, inter-system risk. Access to one IoT device gives cross-sectoral access and can affects IoT systems across different environments (e.g., the "smart" home spreading to the work environment).

3.4 Traditional risk assessment challenges

As a consequence of these changes in the nature of threats, losses, and vulnerabilities, the IoT will require new processes and mechanisms for risk assessments. Risk assessments generally identify, estimate, and prioritise risks to organisational assets and operations, and help to identify options to mitigate, transfer or avoid potential risks (Shameli-Sendi, Aghababaei-Barzegar, & Cheriet, 2016).

Whereas previous cyber risk exposures were mostly limited to digital infrastructures, IoT - due to its cyber-physical nature - can have both digital and physical implications. This interplay requires risk assessments to account for both physical safety and information security, with pre-existing risk assessments having neither adjusted to this variability and scale, nor accounted for the dynamism of interconnected IoT systems.

For example, Lloyd's (2015) business blackout report explored the physical impact of a cyberattack on a US electric grid.

Nurse et al. (2017, p. 25) have highlighted these changes in a recent paper and point to the failure of current methods when it comes to evaluating risk from and to the IoT. The authors consider current risk assessment inadequate, due to:

- Discontinuous periodic assessments. The interconnectedness and variability of IoT systems make periodic risk assessments insufficient because software requires continuous updates and maintenance.
- Fuzzy system boundaries. Assessing and quantifying risk in the IoT is complicated by the lack of clear and continuously changing boundaries between the many devices, services, and complex systems involved.
- Cyber-physical and social blind spots. Not only the information, devices, communication platforms, and interfaces of systems have to be assessed, but so must be the processes, actors, and behaviours through which these devices are being connected.
- Assets as platforms for attack. The technological infrastructures of business are conceptualised as items of value. However, they must also be understood as new possible attack vectors.

3.5 Risk management responses

While the risk management process could potentially be optimised through IoT *(see Section 2)*, detailed requirements to implement best practise are still under development.

Current guidelines frequently leave users without adequate details for implementation (Shameli-Sendi et al., 2016), fail to provide managers with a clear and simple visualisation of the security risk assessment or leave the operational details untouched (Ekelhart, Neubauer, & Fenz, 2009).

Particular challenges include:

- Convergence of safety and security. In the IoT environment, safety and security requirements converge. However, both do not necessarily have the same focus and are sometimes mutually exclusive. This is best evidenced in the automotive sector: Safety targets primarily focus on systematic and random hardware failures, while security approaches focus on attacks that cause unauthorized access and manipulations.

  Besides, vehicle safety assumes that for the sake of a quick analysis and periodic controls, systems resources, such as random-access memory (RAM), should be easily accessed, whereas security would restrict such an access as much as possible, via authentication and authorization mechanisms (Ekelhart, Neubauer, & Fenz, 2009). Future IoT solutions will have to carefully integrate both perspectives.

- Systemic vulnerabilities. Systemic vulnerabilities challenge the management of IoT risk. For instance, the widely shared usage of similar hard and software applications across different manufacturers creates a common but distributed security vulnerability point with wide-ranging influence.

  Thus a single vulnerability in sensors used across diverse sectors and business operations could have similar aggregated effects, the feasibility of which was demonstrated in the discovery of a vulnerability earlier this year in the Intel chips used across an enormous array of devices (Floresca, 2018).

Box 10: IoT risk manager checklist

The IoT Risk Manager Checklist developed by the University of Chicago Law School together with AIG (2017) offers a guide to underwriters to ask particular questions when it comes to risk management in the IoT ecosystem.

The focus is on: autonomous vehicles, home automation, industrial control systems, pharmaceuticals and healthcare devices, smart cities as well as unmanned aerial vehicles.

3.6 Liability

Of further importance for the insurance sector is the question of liability. With the diversity of stakeholders involved in the development and usage of IoT, ranging from manufacturers, software developers, to network and cloud providers, the assignment of liability is becoming increasingly complex. While the IoT is not advancing in a regulatory vacuum (Brass et al., 2018), new technologies invariably present new challenges for existing laws (Boothby, 2014).

Product liability

In particular, the Product Liability Directive (85/374/EEC) is of importance in light of the emergence of IoT. The Directive provides guidance on attribution of liability in the event of damage caused by malfunctioning products. It follows the rationale that anyone who makes a profit from dangerous activities should be held accountable if a danger materialises.

The Directive fulfils a compensatory function and is not only protecting an individual or their property, but also the public and collective interests of society. The legislation applies to all products marketed in the European Economic Area and imposes a liability that cannot be contractually excluded (BusinessEurope, 2016).

Over the course of its 30 years of existence, the legislation has successfully addressed both consumer and producer rights, but its applicability to the evolving IoT ecosystem faces a number of concerns, including the Directive's emphasis on:

– Movable products. The Directive excludes services which means it omits liability for faulty software upon which all IoT products rely;

– Damage. The Directive currently focuses solely on the destruction of items and does not account for non-material damage nor losses derived in the digital environment;

– Proof. The Directive demands that an injured person is required to prove damage by demonstrating a causal relationship between defect and damage. This is aggravated in an IoT environment where software flaws may remain unknown to users.

– Defective. The Directive states that a product is defective when it does not provide the safety which a person is entitled to expect at the time the product was put into circulation. As safety and security concerns in the IoT environment converge and IoT products will have to be continuously updated, the defective notion lacks applicability to the evolving IoT ecosystem.

– State of scientific and technical knowledge. The Directive allows a producer to free him/herself from liability if they prove that they followed the best available scientific and technical knowledge at the time the product was marketed. However, it remains unclear what such a baseline would be in the context of the IoT ecosystem in which software is consistently being added, amended, and improved.

In 2017, the European Commission held a public consultation on the possible need for an update of the Product Liability Directive. The questionnaire specifically focused on the changes that the IoT introduces and was tailored to particular stakeholders and their concerns. Similar to findings by the PETRAS IoT Research Hub, the consultation offered a mixed perspective on the need for a revision or update (Tanczer, Blythe, et al., 2018).

Half of the views expressed in the consultation considered that the current regulatory framework is adequate to address liability issues related to new technological developments, whereas the other half welcomed its revision (European Commission, 2017a). The split in opinion is most prominent between consumer organisations and industry actors, with the latter primarily arguing against the need for any amendments.

As of now, the general consensus seems to be focused on the need to clarify some aspects of the existing product safety and liability regime, for example through guidance documents which are yet to be developed (AIOTI WG04, 2015; BEUC, 2017; European Commission, 2018; Reed, Kennedy, & Silva, 2016; Tanczer, Yahya, Elsden, Blackstock, & Carr, 2017).

However, there is a strong indication that there will be further demands to substantially review the product safety and liability rules as market failures arise through developments in the IoT - especially as machine learning and AI capabilities develop. This will be of particular importance with the expected roll-out of fully autonomous systems such as connected and autonomous vehicles and it signals the need – especially for insurers - to monitor developments and the emerging risk landscape very closely.

Insurers should be aware of the fact that cyber policies may contain exclusions for third-party claims, damages to tangible property, bodily injury, and product recalls. These sorts of liability exposures, however, may be precisely the types of losses caused by a cyber-attack made through the IoT.

Attribution

A final point concerns the question of attribution in the IoT ecosystem, which relates to the identification of responsibility and the allocation of liability for an action or event. Attack attribution has already proven to be difficult in regards to the online context and continues to remain challenging in the IoT ecosystem.

Part of the challenge is low confidence in attribution efforts as a consequence of limited conclusive evidence to pinpoint responsibility for incidents or attacks (Davis II et al., 2017). For researchers such as Rid and Buchanan (2015), attribution is therefore not a binary affair (i.e., yes or no) but a matter of degree. One has to not only draw upon technical/forensic data but also political, and all-source indicators (Davis II et al., 2017).

This has important implications for the cyber insurance marketplace, as most policies exclude acts of war. This could create problems in instances where large-scale deployed IoT systems are targeted by attackers engaging in terrorism or warfare resulting in potentially large economic impacts, but the Terrorism Risk Insurance Act (TRIA) is triggered and insurance coverage issues arise.

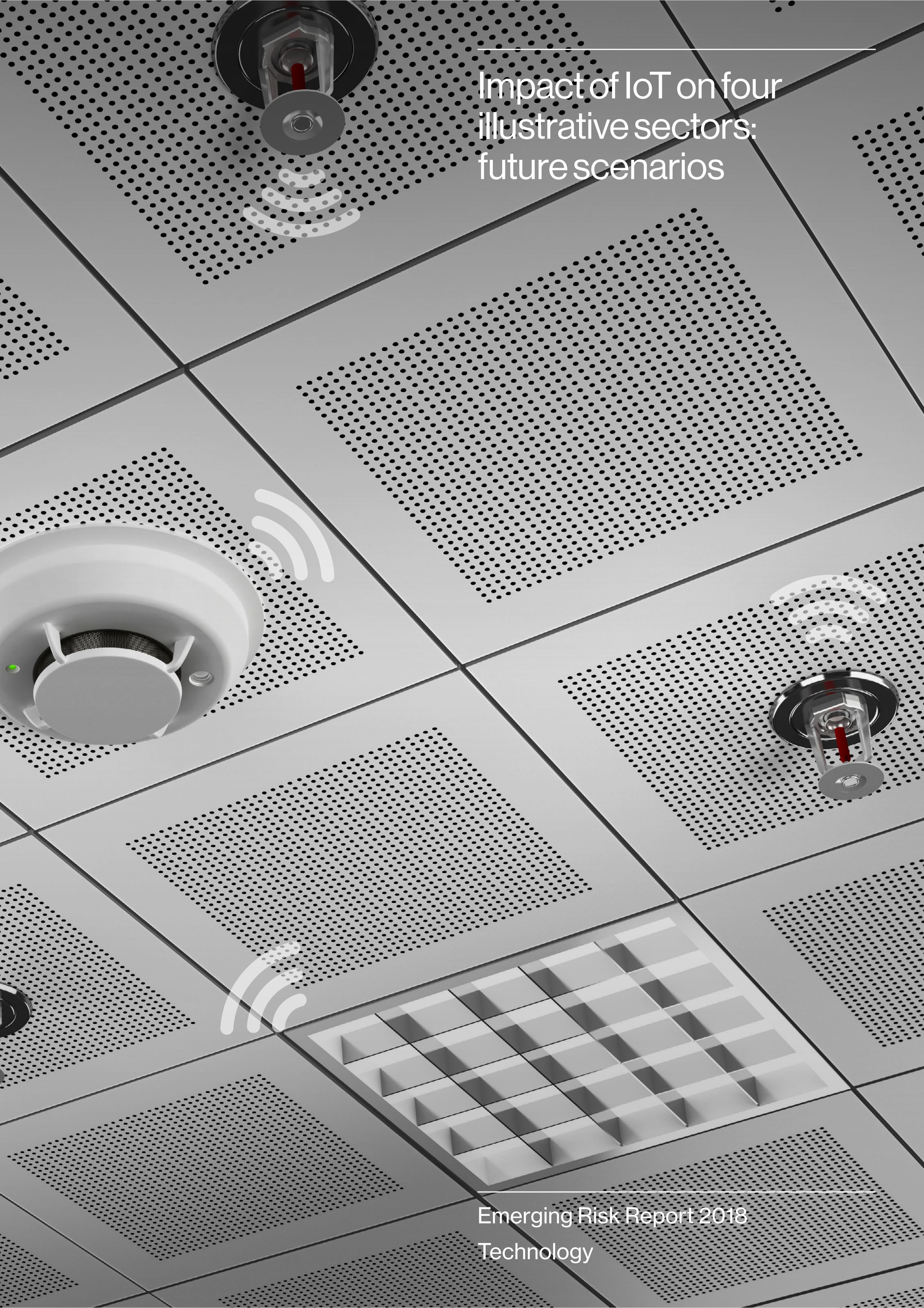
Attribution in the IoT ecosystem will not only be concerned with ascribing an incident to a person (insider threat) or an actor (criminals/terrorists), but potentially a technical fault (e.g. algorithmic bias) within the larger IoT system.

Due to the global supply chain and the heterogeneity of devices and components, the identification and attribution of these incidents will not only become more difficult, but also increasingly more important. The Proofpoint dispute in 2014 *(See Box 11)* demonstrated that technical systems themselves can be (in this case wrongfully) accused of having contributed to a particular incident and attack, opening up the debate about the future risk landscape of the IoT.

Box 11: Blame it on the smart fridge

An example where the problem of IoT attribution became evident was the question of whether smart refrigerators were used to send out spam. In 2014, security firm Proofpoint, claimed to have identified a new security breach that allowed IoT-enabled fridges to be used for an attack campaign (Proofpoint, 2014).

Days later, Symantec criticised Proofpoint's analysis and revealed that the refrigerators happened to be on the same network as infected computers and routers (Thomas, 2014). While in this instance, the IoT system was not the root cause of the spam attack, Symantec also expects that IoT "probably will be to blame in the future".



Impact of IoT on four illustrative sectors: future scenarios

Emerging Risk Report 2018

Technology

4. Impact of IoT on four illustrative sectors: future scenarios

To illustrate these emerging changes to the nature of risks that the insurance market will face, the following section unpacks some of the different risk trajectories across four demonstrative sectors (critical water infrastructure, agriculture, marine, and the smart home).

Using the future to act in the present

- The purpose of the scenarios is to challenge assumptions in order to uncover critical uncertainties.
- They are designed to be extreme (to stimulate creative thinking about risk) but also consistent and plausible[g].
- They intend to support reflection on present practices in order to help insurers to better prepare for the future.

We expect to see profound changes between now and 2030 and we do encourage readers to take the leap and envision both the immediate, mid-term, and long-term effects of IoT. In order to fully realise the potential benefits and opportunities of IoT systems, the insurance industry will have to take up a leadership role. It will be essential to test ideas at an early stage in order to advise on lower risk pathways as the IoT ecosystem expands. The scenarios are therefore set up to help the sector explore IoT's likely impacts and are aimed at helping the industry prepare for these fundamental changes before they happen.

Research approach

To develop these scenarios, the research team pursued a number of avenues (see: Appendix). We first conducted a comprehensive literature review to capture the most up-to-date research on IoT risk projections. We then carried out an expert elicitation survey with 24 respondents. These experts were drawn from the PETRAS IoT research community, industry experts operating within the IoT, as well as wider cybersecurity field, and technology disruption analysis experts.[h]

The expert elicitation survey helped to:

- Identify and categorise the different types of scenarios and risks that these experts anticipate will emerge;
- Engage a wider community of subject experts to better understand current research trajectories; and
- Triangulate the results to ensure the scenarios were representative, robust, and drew out sufficiently complex factors.

All scenarios were further stress-tested in the course of the two expert workshops (one with Lloyd's and one with the Academic Centres of Excellence for Cybersecurity Research). The analysis was then complemented by interviews with Lloyd's underwriters and actuaries.

Scenarios structure

The format of the four scenarios is the following:

- IoT technology by 2030 and beyond. A description of IoT technologies that current research suggests will be potentially deployed by 2030 and beyond;
- Scenarios. The scenario that describes the pathway of how events and risk materialise;
- Risks and critical uncertainties. Critical uncertainties that the scenarios uncover; and
- Impact on insurance. Classes of insurance that may be affected.

[g] Extreme but plausible scenario construction as stress testing devices are a well-known analytical method for future risk management within the insurance industry (see: Realistic Disaster Scenarios; Lloyd's, 2017a).

[h] Some preliminary findings of the expert elicitation survey were analysed and published as part of the PETRAS, IoT UK & IET Conference "Living in the Internet of Things: Cybersecurity of the IoT" conference (see: Tanczer, Steenmans, Elsden, Blackstock, & Carr, 2018).

IoT scenarios

4.1 Critical water infrastructure

As Lloyd's explored in the "Building infrastructure resilience" report (Lloyd's & ARUP, 2017), the water infrastructure supports a variety of other urban systems by providing drinking water, sanitation, heating, cooling, and energy generation. Water infrastructure systems are also dependent upon a variety of critical inputs, including the environments and ecosystems that support water resources and energy networks.

Global investment in water infrastructure is increasing rapidly. The OECD estimates that by 2025, water infrastructure will be the largest recipient of infrastructure investment globally, with spending in OECD and BRIC countries topping US$1trn (OECD, 2007). Yet, increasing demand for water suggests the world may face a 40% global shortfall between forecast demand and available supply by 2030 (UNEP, 2015).

By 2030, the effects of climate change will have significantly increased, resulting in water shortages at particular times of the year[i]. To monitor the usage of this scarce resource, the UK government has rolled out a UK-wide smart and autonomous water and wastewater management system alongside its "Digital Infrastructure Strategy". Water pumps and the UK sewerage network are embedded with sensors that allow for the detection and repair of leaks.

The system makes the network more responsive to user demand, allows for the identification of potential flooding, and is more efficient in terms of used water and pump energy.

Smart transmission network

The UK's potable water network is embedded with IoT-connected sensors and actuators across its pipes, pumps, and valves. These sensors provide comprehensive data streams about the real-time state of assets across the network.

Instead of traditional approaches that monitor the water quality throughout the network using physical samples for laboratory analysis, smart in situ sensors share more accurate and real-time water quality profiles of conductivity, turbidity, temperature, and pH with a centralised analytic platform (Geetha & Gouthami, 2017).

The availability of smart pumps and valves supports real-time pressure responses to fluctuating demand patterns, reducing not only the energy expenditures to maintain sufficient water pressure across the network, but also the frequency of pipe bursts (Bedi, Venayagamoorthy, Singh, Brooks, & Wang, 2018). As sensors now also facilitate the detection of small leak events before large bursts occur, the average operational lifetime of water network assets is increased.

Smart water meters

In the water distribution network, smart meters have been installed at demand points. For the UK water companies, these smart meters provide a more comprehensive understanding of where and when water is used. In times of water shortage, the information is especially helpful for the identification of consumption activities that could be targeted to redistribute peak time demands for water. This not only reduces pump energy costs, but also reduces service disruption events, and allows for the purification of additional water supply.

For both household and commercial users, these smart meters enable an automatic monitoring of water consumption, providing users greater visibility and control over their water bills. Water-powered IoT devices are connected to these meters, such as showers and water taps, and generate real-time information from the centralised monitoring and control system.

Smart meters subsequently can provide advice for water-saving practices. They offer classification of water consumption behaviour for individuals and offer a decision support system deployed as a mobile application in a tablet or any other Internet-connected device (L. Yang et al., 2017).

Smart sewers and flood detection

In addition to the improvement and digitisation of the drinking water system, the UK also continues to retrofit its legacy sewer infrastructure with IoT sensors and pumps and valves. Historically flooding resulted from blockages or overtopping of drainage gullies and manholes following heavy rainfall (Edmondson et al., 2018).

The past two decades pre-2030 saw a significant increase in the frequency and intensity of such flooding driven by changing weather and climate conditions[j]. IoT-supported smart wastewater system now uses real-time integration of weather and water usage data to pre-emptively open network gates and valves. The system redirects sewerage flow surges to areas in the sewer network with capacity, avoiding costly overflows.

[i] Projections for water availability in the UK indicate the possibility of water demand exceeding supply in some UK regions by 2030 (HR Wallingford, 2015).

[j] In 2018, the UK Environmental Agency (2018) has warned of the growing risk of flooding following a pattern of extreme weather events in the previous decade.

Critical water infrastructure scenario: Algorithmic supply bias

Attack

During a hot summer period, the IoT-supported communication networks of water companies is disrupted by an unknown third party.

Impact

Data on remaining reservoir levels and usage intensity is not available. Water supply levels are critically low.

Reboot attempt

Reboot briefly enables the communication network to provide a snapshot of undersupply levels.

Disruption continues

In London, by day three, 40% of customers report occurrence of no water coming through their taps.

Security response

An anti-jamming software patch needs to be installed at each of network's local sensor and actuator hubs due to network's fragmentation.

AI use

AI control system is employed to direct security teams to areas displaying the greatest undersupply levels.

Algorithmic bias

The system, trained on historical usage, is biased and prioritises responses in wealthier neighbourhoods, where households typically consume higher amounts of water.

Disruptions

Poorer areas in London are disproportionately affected, riots start, businesses are interrupted, critical infrastructures such as hospitals face health and safety risks. Local communities sue water companies.

Scenario A: Algorithmic supply bias

During a hot summer period, the IoT-supported communication network of water companies is disrupted ("jammed") by an unknown third party. The jam prevents the IoT central control system from accessing data about the remaining reservoir levels, as well as usage intensity across the networks. Without accurate consumption feedback, control decisions sent to pumps and valves across the network are misaligned. This situation exacerbates the already worryingly low availability of supply levels.

A reboot of the operator's digital control system briefly enables the communication network to function and provides a snapshot of the undersupply levels. However, the attacking activity persists, and as the disruption continues, it becomes apparent that in Greater London the water supply levels are critically low. It materialises that 10% of the network is affected by pressure drops on the first day, 25% on the second day, and by day three 40% of customers report occurrences of no water coming through their taps.

It seems the only way to resolve the security breach is to install an anti-jamming software patch at each of the network's local sensor and actuator hubs. Given the size of the network and its history of disjointed, piecemeal upgrades to its hardware led by different contractors, such a decentralised effort is estimated to take at least 5 days to complete. In order to coordinate the security response, the water companies' AI control system is employed to direct security teams to areas displaying the greatest undersupply levels. As the response mission gets under way, reports begin to come in of dehydration and critical loss of sanitation in some areas. Families head to hospitals for support, but without sufficient water supply themselves, hospitals are faced with aggravated health and safety risks and eventually loss of life.

It transpires the AI system has been trained on historical usage patterns, which biased the system to prioritise responses in wealthier neighbourhoods, where households typically consume higher amounts of water (OECD, 2003), including in recent weeks when the filling of pools provided relief from the heat wave. Consequently, social housing areas across London are disproportionally affected by the attack. Local communities collectively decide to sue the water companies and demand that AI "black boxes" be mandatorily assessed for discriminatory algorithms. Riots erupt across the city and businesses are interrupted.

Scenario B: Smart meter breach

In a move to incentivise customers to use water at "off peak" times, water companies establish a "PlusPoint" system. PlusPoint draws on the water usage data collected from smarter meters deployed in households and businesses to learn about patterns of demand and consumption. It then dynamically highlights times during the day at which changes in those demand patterns could produce energy and capacity gains across the networks. Customers can opt into an alert system and decide to amend their water consumption by, for instance, re-timing their washing machine or dishwasher. Users who employ this time-sensitive water service are rewarded with PlusPoints that can be collected for deferred cost deductions from their bill.

The PlusPoints market is opened up to vendors beyond water providers, and points can now be traded for consumer items such as discounts on cinema tickets or early views of new fashion collections[k]. These features significantly boost the popularity and uptake of the trading scheme. Behind the scenes, smart meters use an open application programming interface (API) for any (certified) company to provide their own version of an AI-driven software agent to seamlessly trade a user's unused PlusPoints for features of their liking. Many companies provide different types of these software agents and they are tested, reviewed, and ranked by industry watchdogs.

News emerges that some of the software agents used to trade PlusPoints have a substantial security flaw that has leaked personal household data from the sensors. While the water companies deny these allegations referring to it as "fake news", some consumers stop trading their PlusPoints nevertheless. After a few days, the business models of some of the software agents are affected, and when news breaks that some are considering withdrawing from the scheme, many more consumers decide to stop trading.

Seemingly overnight, water companies are inundated with customer requests to have their PlusPoints paid out on their water bills. Not only does this result in an extraordinarily high and unexpected cost, but water companies also observe reputational damage and a behaviour switch by customers back to using more water at high peak times, further adding to the operational costs and undersupply concerns of the network operators.

[k] Similar schemes to incentivise redistribution of peak demand on network-based services have been employed primarily on transit infrastructure, such as Hong Kong's linked Perx reward scheme with its EZ-Link commuter card (EZ-Link, 2018).

Scenario C: Water bio-terrorism

During a longstanding dispute between two nation states, alleged state-affiliated actors attack one of the primary national smart filtration sites in one of the two countries. The attackers compromise the operational system and modify the algorithms translating measurements of microbiological contents, chemical agents, and pH levels of water into treatment commands in the final stages of the purification process[l].

To disguise the breach, the attackers modify the dashboards used to monitor the water quality parameters. These continue to display levels that meet drinking water standards, even as the actual levels begin to surpass safety thresholds.

The attack is first suspected when IoT sensors belonging to a sewerage system operator detect anomalies in a region's water pH levels. The sewerage company rapidly collates their sensor readings and shares these with other critical infrastructure operators to mobilise a forensic investigation and locate the breach.

When the compromised plant is identified and secured 24 hours later, the government calls for an assessment of the extent of civilian casualties and commercial losses. The assessment is inconclusive and lawsuits follow from manufacturers who had to discard food products produced at industrial plants suspected of having been affected by the contamination

Critical uncertainties and IoT's impact on insurance for future risk management

Unclear attribution. Existing legacy security issues in IoT device design, emerging algorithmic code vulnerabilities, and the likelihood of future disruptions by erroneous longitudinal data use will complicate the attribution of harm. What attribution protocols will be needed when it is not possible to clearly identify the intentional or unintentional nature of harm?

Cascading and aggregated risk. Due to interdependencies, IoT systems propagate cascading risks. It then becomes hard to quantify the resultant reputational damage affecting affiliated companies and to establish who is liable for the outages caused by IoT failures.

Algorithmic biases. AI systems that learn from data inputs and machine learning techniques will become more widespread as IoT systems become more pervasive across critical infrastructure networks. As severe disadvantages or adverse outcomes can result from potentially biased decisions taken by such AI systems insurance will need to start thinking about product to cover the risk and impact of biases.

Impact on insurance. Multiple classes of insurance will be affected across the critical infrastructure sector as different types of threat and losses become more closely connected. These will include errors and omissions, general liability, business interruption, cyber, terrorism, and property.

[l] While drinking water has been widely treated as critical infrastructure for nearly two decades, events including the 9/11 attack on US soil have led to significantly heightened attention to the security of water utilities (Bitton, 2014; Meinhardt, 2015). The potential impact of IoT devices in bioterrorist attacks is also an emerging field of preparedness.

4.2 Agriculture

The year is 2030 and IoT-connected farm sensors and actuators are commonly used throughout the global agricultural sector. In the wake of decades of the large-scale application of pesticides and chemical fertilisers, farmers have been experimenting with emerging technologies to counteract legacy pest and pathogen resistances. They also hope for these systems to bring down high operational costs and to address widespread losses of soil biodiversity.

As was anticipated by experts, it was the partnering of IoT with emerging nano-encapsulated fertiliser technologies, that truly accelerated a first “wave of IoT adoption” (European Commission, 2017b).

A series of materials and manufacturing innovations removed the prohibitive cost of IoT devices and IoT-driven farming is now capable of offering competitive benefits even in major agricultural markets where farm labour costs had been historically low.

The relentless influence of wider systemic pressures on the agriculture sector, including increased global food demand, water shortages, stressed land productivity, and volatility in weather conditions, has cemented IoT as the new operational paradigm for farming worldwide (Tzounis, Katsoulas, Bartzanas, & Kittas, 2017).

Remote and algorithmic farm operation

In the pursuit of economies of scale when faced with significantly reduced land productivity, the agricultural sector slowly transitioned to predominantly large, cross-national farming corporations.

Sensors, drones, autonomous tractors, and other farm robots are remotely controlled from command centres often not even based within the same national administrative boundaries (Braun & Schreiber, 2017).

These industrial control centres are the hearts of the sectors. Most of the labour employed in agriculture now comprises data analysts and algorithm programmers in search of data-based means of achieving better yield, less waste, and reduced theft. Performance has exceeded the historic estimations of 25% better yield per crop and 25% reductions in weather-related harvest damage since their adoption (Bayer, 2018).

With many farming corporations employing the same technologies, competitive advantage is largely derived from innovative integration of algorithmic farm management with market demand signals[m]. Agricultural data control centres are linked into predictive consumer demand markets and adjust livestock and crop harvesting on an hourly basis.

At national level, largely concerned by maintaining influence on the global food price markets, a national government makes agricultural subsidies and climate risk grants contingent on minimum levels of IoT deployment.

Precision crop farming and individual livestock management

Sensors are deployed across crops, soil, and the atmosphere to capture high resolution data on levels of soil moisture, soil nutrients, plant water usage, plant growth, and weather conditions. This data is used to monitor early outbreaks of diseases, detect leaks in irrigation systems, design custom fertiliser profiles, and model predictive local microclimate conditions.

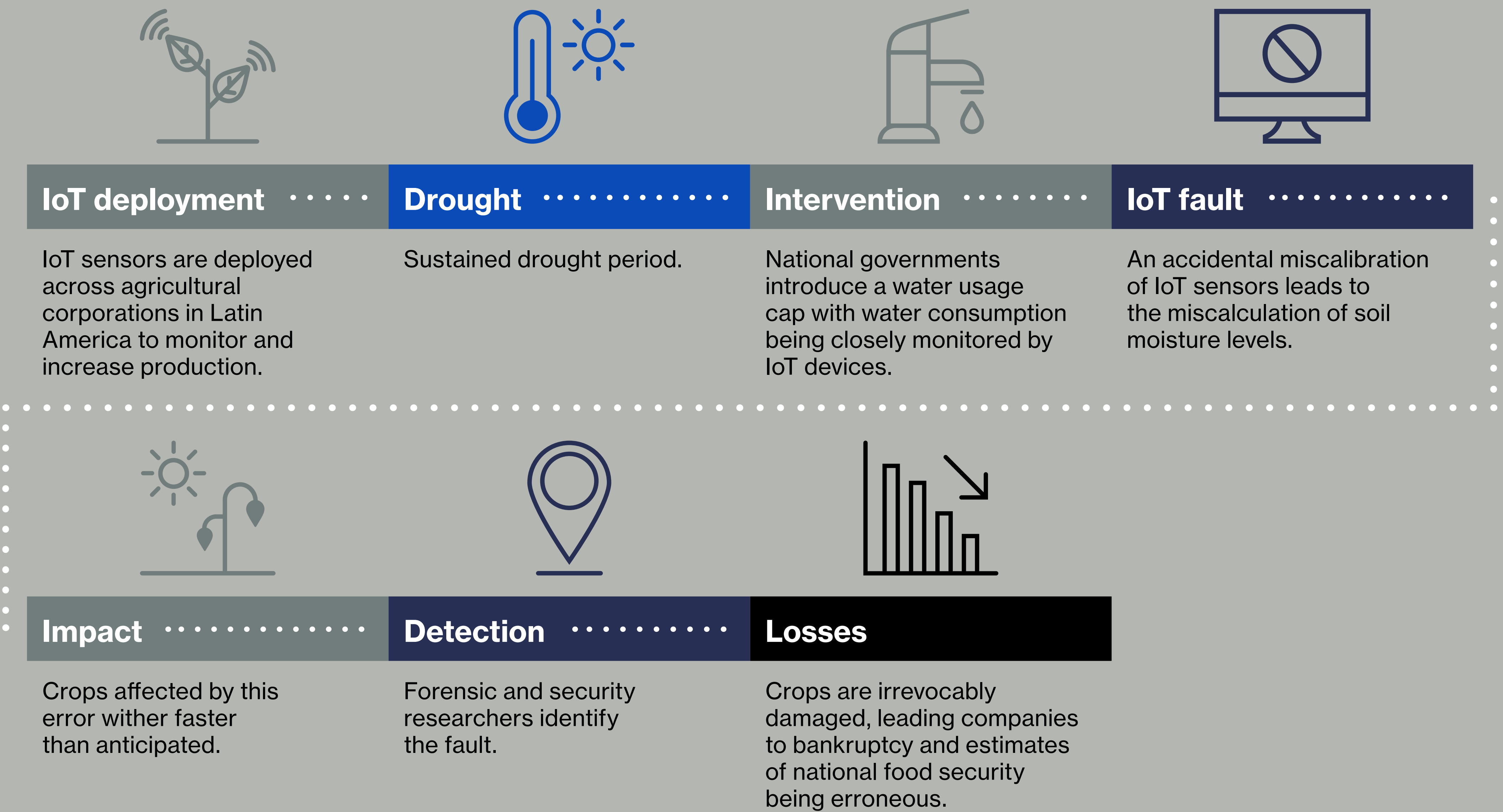
These data streams are integrated by decision algorithms that manage autonomous robots in choosing the optimal times to plant, irrigate, feed, and harvest (King, 2017). Many farm corporations are working around accuracy parameters of a few centimetres and extensively employ “extreme patchwork” in their operations, where fields that used to be single crop now host many different varieties throughout.

Following material innovations, IoT devices can be powered for at least as long as the lifespan of the livestock monitored. All livestock including cows, pigs, poultry, etc., is now monitored individually with bolus-ingested sensors and RFID movement monitoring tags. Data is collected on animal location, speed of movement, health, pregnancy status, feeding levels, etc.

The adoption of IoT has led to a step-change in avoidance of stock contamination by disease, as well as reduced the operational cost of antibiotics usage on large livestock groups, and the hefty fines for breaching bacterial resistance protection standards introduced a few years ago (King, 2017).

[m] In a recent Lloyd’s (2018) report on exploring crop (re)insurance risks in India, the merging of technologies such as IoT and AI showed to improve loss adjustment and assessment. For instance, the value of probabilistic crop models providing a mechanism to integrate and synthesise all the relevant science and data into algorithms can expand 20+ years of past historical experience to thousands of years of modelled data. This enables a better understanding of potential pathways and probabilities of loss events occurring.

Agriculture scenario: Miscalculation of soil moisture leads to crop losses



IoT deployment

IoT sensors are deployed across agricultural corporations in Latin America to monitor and increase production.

Drought

Sustained drought period.

Intervention

National governments introduce a water usage cap with water consumption being closely monitored by IoT devices.

IoT fault

An accidental miscalibration of IoT sensors leads to the miscalculation of soil moisture levels.

Impact

Crops affected by this error wither faster than anticipated.

Detection

Forensic and security researchers identify the fault.

Losses

Crops are irrevocably damaged, leading companies to bankruptcy and estimates of national food security being erroneous.

Scenario A: Miscalculation of soil moisture leads to crop losses

IoT sensor are deployed across agricultural corporations in Latin American countries to monitor production and to reduce the uncertainty surrounding the impacts of an extreme shock to the food supply chain (Lloyd's, 2015). It is believed that increased data streams and greater data aggregation will facilitate more effective and proactive crop management.

During a sustained period of draught, the national government introduces a water usage cap with water consumption being closely monitored. As a major consumer of water, the agricultural sector is under especial scrutiny. Exceeding the stipulated limits results in farmers having to pay fines.

As the drought continues, one Ministry of Agriculture elevates the national food security alert to "critical". The government decides that as a matter of national security, it should be able to closely monitor the crops' status and growth and have access the data streams of the agricultural corporations.

Additionally, in order to protect some of the remaining crops, selected farmers should be allowed to exceed the stipulated water use cap. The ministry therefore decides to use the collated information to forecast crop irrigation needs and determine when and which farmers will be allowed to exceed approved water consumption levels to guarantee food security.

An accidental mis-calibration of IoT sensors by a commonly deployed manufacturer leads to the miscalculation of soil moisture levels. The levels are in fact lower than the reading shows. Crops affected by this error wither faster than anticipated. By the time the fault is detected, crops have already been irrevocably damaged, leading companies to bankruptcy, estimates of national food security being erroneous, and insurers paying out for the large loss.

Scenario B: US remote-sensing crop hacking

In 2030, crops are fully machine operated and harvested without the need for a single human labourer in the field. Satellite data is used to monitor crop, and remote sensors control land quality and water resources while big data analytics optimise production with resource availability.

Organised anti-GMO collective compromise several agriculture management systems used by large, listed US companies. They manipulate the data collected by the companies' sensors over a three-month period. When the breach is discovered, all the data held by the management systems is considered corrupted and is shown to be unreflective of the real status of yield.

Automated farming is interrupted and companies react by sending workers and tractors out to manually measure parameters, assess crop readiness, and continue planting. Given the scale of operations and the loss of precision capability, planting capacity is reduced by 50% (Public-Private Analytic Exchange Program, 2018).

Agricultural companies see their income being impacted and incur in additional expenses as a result of the impaired functionality of management systems. This event erodes confidence in companies' stocks prices affecting both European and Asian markets and global food resources.

Scenario C: Automated milking

In 2030, large dairy companies in California, Wisconsin, Idaho, New York, and Pennsylvania[n] are fully automated. Automation includes robotic milking machines, as well as IoT sensors to monitor and adjust the environment of the barn housing the herd. The failure of the IoT sensors managing the barn environment results in a dramatic shift in temperature that compromises long-term health to the herd and leads to loss of milk production.

Critical uncertainties and IoT's impact on insurance for future risk management

Data formats. To ensure interoperability across deployed IoT systems and to make use of the breadth of data streams, standardised data formats will be needed. How can the value of IoT and its data be suitably assessed if the data capture across these IoT systems significantly differs?

Trust in data. IoT systems become more pervasive and embedded in critical sectors that are used to make complex, anticipatory decisions based on automated IoT data streams.

Impact on insurance. The classes of insurance that would be affected are agriculture and schemes' reinsurance, business interruption, contingent business interruption, cyber and political risk.

[n] These are the top 5 dairy-producing states, accounting for 50% of US's production (Goodling, 2016).

4.3 Marine

Following an initial period of tentative scepticism, the benefits of connected and autonomous vehicles (CAVs) on land have led the shipping sector to follow suit by implementing autonomous vessels[o]. In 2040, cargo is largely delivered by autonomous, unmanned ships[p] which carry IoT-supported freight that is loaded and unloaded at autonomous ports. IoT sensors allow for the continuous accurate tracking of autonomous ships route and condition. Cargo can be monitored 24/7 and information about the temperate, location, humidity levels etc. is collated.

Autonomous ships

Previously, human error accounted for approximately 75% of marine liability losses (Allianz, 2017). By 2040, such errors have been largely reduced though not entirely eliminated by a transition to autonomous navigation of marine vessels (Barthelsson & Sagefjord, 2017).

Shipping is not without risks, and years of research focused on developing cost-benefit evidence bases to explore unknowns in the areas of collision events, cybersecurity, and safety in absence of crew, the ship's ability to respond to disasters, and compromised system reliability.

Over time, pilot project demonstrated both improved shipping safety, as well as cost-reductions[q]. Crew pay and its accommodation costs have decreased and profit margins increased (Kretschmann, Burmeister, & Jahn, 2017).

Removal of workforce from ships also enhanced the efficiency of space use for cargo, and on board consumption of energy, garbage management, and treat sewage, (J. Yang et al., 2018) but also eliminated the mental health problems common amongst seafarers (Sampson, Ellis, Acejo, & Turgo, 2017).

Real-time, remote control

Autonomous ships use real-time weather information as well as pressure, temperature, and wind speed data to optimise the fuel consumption and total journey time of their routes (J. Yang et al., 2018). The ships themselves are electrically powered[r], to reduce the possibility of oil spillages and related other environmental damages. IoT-supported solar as well as wind systems help to provide additional energy sources.

These features support the global climate ambitions of the maritime industry (Government Office for Science, 2017). Technology has progressed to be able to ensure the high bandwidth data transfer via satellites which is necessary for constant connectivity (Government Office for Science, 2017).

This is particularly important for obtaining vessel performance data to increase precision and enhance certainty. Predictive maintenance, confirmation of turnovers and real time verifiable data about the location of cargo are some of the other advantages that automation in the maritime sector has provided.

Box 12: Will autonomous vessels be safer?

A study by Wróbel, Montewka, & Kujala (2017) analysed 100 maritime accident reports and assessed whether the introduction of unmanned ships would change the rate of accidents as well as their consequences.

While the analysis was limited to safety hazards and did not account for intentional actions (piracy, terrorism, etc.), the research showed that the introduction of autonomy and the removing of crew members can decrease conventional accidents' probability; especially in events in which humans' actions had a direct impact on its occurrence.

Any arising accidents, however, may lead to more severe consequences without a crew to intervene. Consequently, they found that unmanned vessels would perform better in reducing the likelihood of accidents than they would in mitigating the consequences when an accident did occur. Thus, it is important to note that while autonomous shipping offers numerous benefits, further research and discussion are needed with all parties to ensure public acceptance, regulatory compliance, and safe operations in a fast changing marine environment.

[o] Rolls-Royce (2016) expect that fully autonomous unmanned ocean-going ships will be available by 2035. KONGSBERG is currently also in the process of building a fully electric and autonomous container ship YARA Birkeland that is to be launched in 2020 (Matthews, 2017).

[p] Lloyd's Register has proposed six autonomy levels (AL) for shipping to provide clarity to shipping stakeholders of the specific requirements of different automation strategies. These range from AL1 for ships with data collated for on board decision making, through to AL6, which denotes a fully autonomous ship with no access required during a mission (Lloyd's Register, 2016).

[q] Crew costs can vary from around 10% to 30% of ship-owners operating expenditure (Allianz, 2017).

[r] The first electrically powered ship is to be tested in autumn 2018 (Futurezone, 2018).

IoT-supported cargo and semi-autonomous ports

Cargo is part of a larger IoT-enabled supply chain that makes the real-time monitoring of goods possible. This is particularly helpful for the transport of perishable goods and livestock. The vessels transport IoT-supported containers to enable real-time tracking of the location and condition (e.g. temperature) of individual cargo items[s]. Dependent on the content, containers are equipped with cooling or humidity sensors as well as Radio-Frequency Identification (RFID) tags.

The effective use of autonomous ships and IoT-supported cargo is enabled by the development of semi-autonomous ports that use blockchain technology to secure containers[t]. This has required a shift in skills of both the marine and port workforce (Government Office for Science, 2017).

Box 13: IoT-supported transport of goods

The use of IoT supported vessels and containers can better support the transport of perishable products. For example, Denmark's Maritime and Commercial Court found a shipping line liable for damage to a $282,000 consignment of frozen sushi in transit from Hamburg to Copenhagen after the vessel was caught in heavy weather and high seas.

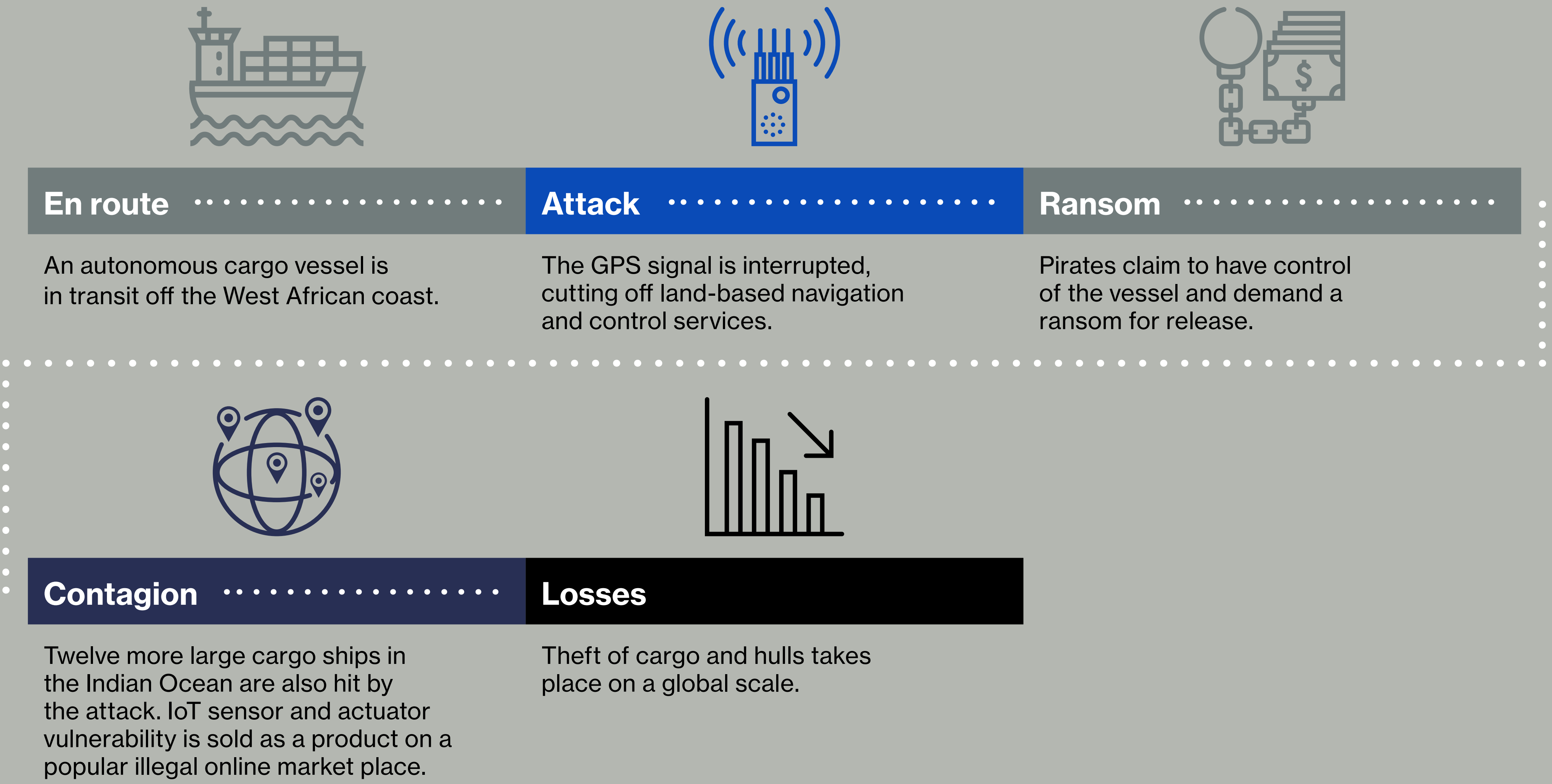
The ship's cooling system suffered damage, resulting in the cargo being subjected to a variation in temperature between -10.9C and 15.8C. Although the carrier defended the claim on the basis that the goods had been cleared by the food health authority and that it could not be held accountable for the bad weather which caused the damage, the court rejected the defence on the basis that the vessel had departed Hamburg well aware that weather forecasts predicted conditions which varied between strong gales and storms (van Marle, 2018).

In the future, improved weather data collated from IoT sensors and fed back to autonomous ships may offer an ability to proactively identify and consequently mitigate such risks in order for shipping lines to make fully informed decisions.

[s] In 2018, Maersk and IBM announced their intent to establish a joint venture to provide more efficient and secure methods for conducting global trade using blockchain technology (Maersk, 2018).

[t] The Port of Antwerp already relies on blockchain technology for the tracking of containers (Marsh & BRINK, 2017). However, the security of the Antwerp Port IT Systems has already previously been compromised resulting in information breach, and on-premises theft of containers and disruption (Bateman, 2013).

Marine scenario: Hacking and vessel piracy



En route

An autonomous cargo vessel is in transit off the West African coast.

Attack

The GPS signal is interrupted, cutting off land-based navigation and control services.

Ransom

Pirates claim to have control of the vessel and demand a ransom for release.

Contagion

Twelve more large cargo ships in the Indian Ocean are also hit by the attack. IoT sensor and actuator vulnerability is sold as a product on a popular illegal online market place.

Losses

Theft of cargo and hulls takes place on a global scale.

Scenario A: Hacking and vessel piracy

An autonomous cargo vessel is en route off the West African coast. The vessel's GPS signal is interrupted and all contact to land-based navigation and control services cut off. The vessel's operator is contacted by pirates who claim that they are both physically and digitally in control of the vessel and demand a ransom payment for release of both vessel and cargo.

The next day reports surface of the same scenario having been encountered in the Indian Ocean, already having close to a dozen large cargo ships. By the end of the day, experts report that vulnerability in the IoT sensors and actuators used as part of autonomous shipping navigation system was exploited by tech-savvy criminals and recently advertised and sold on a popular illegal online market place as a product to pirates. Theft of cargo and hulls takes place on a global scale.

Scenario A: Cargo sensors disputes

An IoT-supported cargo vessel[u] transports perishable goods from Saldanha Bay in South Africa to Felixstowe in the UK. As part of normal practice, a surveyor assesses and approves the condition of these goods on behalf of the cargo operator at the time of departure.

Throughout the journey, IoT sensors relay data about the temperature and moisture content on-board the ship and its containers to a remote monitoring system at the cargo operator's headquarters in India, but no alert signals are seemingly triggered or received.

Upon arrival in the UK, however, the goods are found to be spoiled and damaged. The data feeds from the IoT humidity and temperature sensors as well as the on-board video footage are checked for anomalies during the journey. No immanent fault is identified.

A subrogation dispute arises and the insurers of both the ship's and cargo's owners draw on the expertise of different cybersecurity companies to investigate the case. When the experts come to different conclusions - a human error introduced during routine maintenance by one and a structural failure of management systems by another - a lawsuit follows.

Scenario C: Variable route premiums

The insurance sector sees a shift towards more widespread use of automated on-off payment systems. IoT-supported sensors are employed to create dynamic assessment of threshold boundaries on heightened exposures to different risk, whether driven by changes in weather, economic activities, or social interactions.

In the maritime sector premiums go up for periods during which ships sail through a high-risk area or berth at ports characterised statistically by greater levels of insecurity. Premiums decrease again once a ship has passed a certain dedicated zone or port.

As a consequence, this new approach to insurance models especially increases costs for goods in particular countries. Affected nation states come together and sue major insurance providers for inadvertently disadvantaging them and hindering their international trade prospects.

[u] While "intelligent" cargo concepts are not new (see: Forcolin, Fracasso, Tumanischvili, & Lupieri, 2011) and will be readily available before 2030, the large-scale realisation of a fully IoT-supported supply chain logistic will take years to find implementation.

Critical uncertainties and IoT's impact on insurance for future risk management

Subrogation disputes. The IoT is adding value to the international shipping and cargo sector through the ability to monitor systems and to identify failures and resolve claims. However, uncertainties remain. IoT might decrease emerging subrogation disputes, but also complicate the identification and attribution of failure. The insurance industry will have to consider how long will cyber exclusion policies such as "CL380" (the most widely-used exclusion applied across all marine lines and included on some policies in the bloodstock/livestock, general liability, onshore energy, political risk/political violence, power generation and UK commercial property markets) (LMA, 2018) be retained in this emerging IoT environment.

Infrastructure and legislative demands. As autonomous ships sail across international waters and berth at ports in different jurisdictions, it is unclear how ship owners and container operators will remain compliant with regulatory demands across diverse jurisdiction. What the transition period will look like until international agreements or legislative frameworks (e.g., data exchange) are set in place, as well as suitable port infrastructures are completed is to be understood. Regulatory uncertainty and different level of adoption might have an impact on business continuity, safety, and security.

Changing nature of threats. While IoT systems allow for higher precision and better maintenance of vessels and cargo, threat actors will correspondingly adjust their attack portfolio and skill sets. Piracy and theft risks will change in future autonomous shipping environments.

Impact on insurance. Multiple classes of insurance will be affected, as the same vulnerability in an IoT supported vessel can generate different outcomes across different lines - including marine cargo, hull, cyber, war (piracy), property, business interruption and liability.

4.4 Smart home

The year is 2040 and practically all homes have Internet-enabled sensors and actuators embedded in both large and small household appliances, as well as building's physical infrastructure. Smart technologies' perceived usefulness and their increased affordability and integration levels are fostering IoT adoption rates (Adapa, Nah, Hall, Siau, & Smith, 2017; Hsu & Yeh, 2017).

Functionalities range from self-adjusting mattresses that regulate sleep patterns and sleep quality (Dijk, Liang, Zhang, & Hu, 2017; Pimenta, Chaves, Fernandes, & Freitas, 2017), to smart wardrobes that suggest outfits based on weather data, calendar information, and user habits (Perry, 2016), to laundry machines that sense the nature of clothes and optimise settings accordingly.

Convenience and well-being enhancement

Automation household and entertainment systems dominate the commercial market and humanoid robots have begun to be deployed for domestic tasks (Charara, 2018). While IoT was originally perceived as desirable for its ability to enable health benefits, energy saving, and financial gains through household expenditure management (Longe & Ouahada, 2018), families now equally invest in IoT systems that enhance leisure and comfort, and reduce household labour and inconvenience (H. Yang, Lee, & Lee, 2018)[v].

Users have developed an expectation that systems are remotely controllable, fully autonomous, and provide simplified interfaces. For example, to ensure a good living or sleeping environment, IoT-supported household systems including the heating, TV, or couch sense resident's movement, gestures, body temperature, as well as voice levels. The gathered information can be used to assess an individual's current condition, including the identification whether a person is awake or asleep.

Knowledge about the state of the person enables IoT and AI systems to adjust settings, helping to increase comfort levels of family members (Feng, Setoodeh, & Haykin, 2017).

Smart family management

By 2040, IoT is a constant feature in the management of personal and family life. Though initially met with scepticism about the blurring of work-home life boundaries and concerns about privacy, safety, and distraction, IoT has gathered substantial momentum. Interdependent and Internet-connected systems are used in care settings ranging from infants to elderly family members (Binu, Akhil, & Mohan, 2017; Gaspar, Bonacin, & Gonçalves, 2018).

In particular, young working parents draw on IoT devices to find a better work-life balance and to receive additional childcare support. In this future environment, the sound of a baby crying triggers an automated temperature adjustment, movement simulation, and feeding control (Y. Yang et al., 2017).

Location-tracking technologies are used to enhance security and safety while children play in neighbourhood parks, with wearable devices suggesting to them to complete their weekly exercise routine for their school sports team. Busy parents use arrival notifications and augmented reality features to welcome their children home from school, allowing them to simultaneously finish off final tasks at work.

[v] A study by Ghaffarianhoseini et al. (2013) theoretically analysed case models of smart houses (e.g., MIT Smart House, Toyota Dream House Papi) in order to identify their essence and characteristics. Their results show that the most significant intelligent values embodied in smart houses embrace technologies that allow automation and ensure a comfortable living environment. Since its publication in 2013, more smart home demonstrators have been established, including in the UK (e.g., Building Research Establishment in Watford, PETRAS IoT Research Hub). These models are important test-beds to not only envision but to inquire the future of smart home automation.

Smart home scenario: Psychological harm

Smart family management

IoT-enabled “smart family management” is perceived to support working parents in achieving a better work-life balance.

Impact

After a few years, parent-child relationships have been critically impacted and emotional and cognitive child development impaired.

The skills that were historically touted as the critical economic competitive edge of certain nations are now systemically lacking.

Social concerns

At a national level, there are concerns about the implications for the competitiveness of the labour force.

Evidence emerges

An influential piece of research emerges that claims a clear influence of IoT-dependent activities on social developments.

Legal actions

Legal actions emerge in the US looking to attribute responsibility for the long-term harmful impacts of IoT.

Scenario A: Psychological harm

Initially the usage of IoT-enabled “smart family management” is perceived to support working parents in achieving a better work-life balance. After a few years, however, it seems that parent-child relationships have been critically impacted and emotional and cognitive child development impaired. Symptoms include reports of widespread experiences of increased detachment by children, depression and isolation, lack of demonstration of independent problem-solving and low levels of creative reasoning.

At a national level there are concerns about the implications for the competitiveness of the labour force. The skills that were historically touted as the critical economic competitive edge of certain nations are now systemically lacking – including social collaborative skills, enhanced cognitive problem-solving and deep creativity. An influential piece of research emerges that claims a clear influence of IoT-dependent activities on social developments.

A niche, but rapidly growing industry of legal action firms emerges in the US looking to attribute responsibility for the long-term harmful impacts of IoT-enabled households on individuals. The press is replete with stories of children suing their parents for negligence; parents mobilising on behalf of their children against IoT manufacturers; and even large employer organisations exploring actions against the government for failing to step in sooner.

Research on the impact of Internet, smartphone, and tablet usage on children (i.e. regarding the effect portable and instantly accessible source of screen time has on children’s learning, behaviour, and family dynamics) has lagged considerably behind the rate of its adoption (Radesky, Schumacher, & Zuckerman, 2015).

A systematic review of the literature on problematic Internet usage by adolescents and adults summarised the existing longitudinal evidence (Anderson, Steen, & Stavropoulos, 2017). It showcased how behaviours of problematic or excessive Internet usage do occur and can result in negative outcomes for the concurrent and the future adaptation of young individuals.

Box 14: An automated self-certifying security scheme for future smart home devices

To deal with the growing diversity of IoT home systems and their need for frequent software updates, in the future an automated IoT “security certification scheme” may be rolled out. Similar to known procurement guidelines (e.g., UK Cyber Essential) and prior research on dynamic certification (Lins, Grochol, Schneider, & Sunyaev, 2016), the scheme may list IoT products in a blockchain-supported database that features products that have been tested prior to market entry and verified to fulfil clearly defined safety and security standards.

The listed IoT vendors can commit to continuously update and, thus, re-certify their systems, with the information about each product’s security status being made immediately available online through the database.

New IoT products may be designed to automatically draw on this database to request information about the security status of other IoT products within the system they operate in. They can use this information to decide whether or not it is safe to share data with another product, with the system flagging potential vulnerable IoT systems to home owners.

Users can thereupon verify the systems security status and either extract the vulnerable IoT node or manually override the decision. They may also choose to report when IoT products and services are erroneously flagged insecure. This measure may clarify responsibilities in the IoT ecosystems as users are found to frequently ignore requests for software updates (Fagan, Khan, & Buck, 2015) and, conversely, many IoT vendors do not offer long-term software support.

While the automated scheme discussed here remains futuristic and requires further research, the EU is currently building a voluntary certification framework for information and communication technology (ICT) services which will also affect IoT systems. On 8th of June 2018, the Council agreed to the Cybersecurity Act (European Commission, 2017a) and is in the process of preparing for negotiations with the European Parliament to finalise the text.

Critical uncertainties and IoT’s impact on insurance for future risk management

Liability and certification. It is now commonly assumed that users cannot be expected to accept responsibility for the malfunctioning of IoT devices in their home. In the future when collective IoT system may start making harmful decisions this assumption might not hold anymore and the question of attribution and liability will be a very important one.

Preferential security premiums. IoT manufacturers will seek to achieve a “certified” security status but may fail to anticipate all potential data breaches and product failures. New type of considerations should inform “trusted IoT design” schemes to guide consumer-manufacturer liability agreements.

Emerging types of harm. In changing social and economic interactions, the IoT is likely to give rise to damages and losses (such as psychological harm) that are currently not yet accounted for in risk models. The time frames within which these impacts might not be currently considered sufficiently to manage long term risk exposure resulting from IoT deployment. Mental health research might not be able to tie back specific harms deriving from emerging technologies to a specific cause.

Impact on insurance. The classes of insurance that would be affected include directors and officers, product liability, and general liability.

Implications for the insurance sector

Emerging Risk Report 2018
Technology

5. Implications for the insurance sector

As recently as 2016, Ernst and Young referred to the IoT as a “futuristic concept” and suggested that many insurers were adopting a “‘wait and see’ attitude” (EY, 2016). In the two years since that report was released, the usage of IoT has increased and insurers are looking at the emerging risks and compelling value propositions that the IoT generates. The scenarios developed in the previous section highlight some areas of systemic IoT risks and raise important considerations for new business models, the operational future of underwriting, insurance claims, and modelling. In order to capitalise on this transformation, the sector will have to move quickly and recognise opportunities and challenges in order to lead the way and avoid being left behind. To capture this potential, the insurance sector may take the following aspects into account (*see Table 1, below*):

Table 1: Benefits and operational requirements for the insurance sector

What will IoT allow	What will IoT require
− Generate granular and real-time data	− Holistic solutions to meet customer needs
− Capture patterns and behaviours	− Shift in insurer’s product portfolios
− Change ownership patterns	− Increase in coverage
− Enable proactive monitoring	− Blended cyber/physical rating models
− Improve risk understanding	− Strategic third-party collaborations
− Enhance loss management	− Changes to risk assessments
− Avoid preventable losses	− Changes to security questionnaires
− Tackle information asymmetries	− Standardised policy language
− Reduce the number of claims	− Standardised data capture
− Gamification of processes	− Advanced data science talent
− On-the-go insurance models	− Ethical framework for IoT data usage

5.1 Business models

In addition to changes emerging from the influx of directly available, unfiltered, and granular data streams described in the scenarios, the IoT also provides the opportunity to personalise policies and offers. This enables the insurance sector to automate decision making and to improve the premium calculation of risks in diverse sectors. The IoT further contributes to the growing interest in the cyber insurance market, which reached an estimated 3.5 billion USD in written premiums in 2016 (OECD, 2017) with premiums having steadily grown at a rate of roughly 30% every year for the last five years (Aon, 2017).

Usage-based insurance

Usage-based insurance (UBI) or so-called “pay-as-you-live”, “on-the-go”, or “pay-as-you-drive” insurance policies (EY, 2016, p. 4) are becoming more popular as a consequence of the IoT and AI. These UBI solutions are particularly promising for the motor insurance sector, where telematics have taken off.

IoT UK has highlighted that the road-market segment is poised to experience a rapid growth in this regard (Griffiths, 2017) with the US, Western Europe, Japan, and the BRIC nations expected to dominate the sale of new cars with embedded measurement technologies (EY, 2013).

Telematics and associated UBI's have substantial benefits for the insurance of fleets, including trucks, and delivery vans. Such technologies are able to facilitate better risk management, modelling and, consequently, more accurate policies in terms of coverage and pricing, in the transition period until fully autonomous vehicles dominate the traffic (see Box 15).

Together with this, the monitoring of drivers through UBI could potentially create or enhance a benign incentive, by partially transferring the power of pricing to the policyholder, discouraging reckless driving behaviours. Likewise, this extra incentive could eventually reshape the role of traditional insurance clauses such as deductibles and warranties, which are normally devised to control the policyholder's behaviour when it cannot be fully monitored.

Box 15: Telematics

Telematics describe in-vehicle measurement technologies that can serve as an underwriting tool to improve loss experience, including claims management, servicing, and acquisition.

Such "black box technologies" collect information on the performance of a driver. For instance, UK-based black-box provider and insurance brand Ingenie assesses how a person drives in four key areas: speed, braking, acceleration, and cornering.

Drivers receive feedback on their driving via an associated mobile app or online platform which points the user into the direction towards lowering the cost of their car insurance.

A study by Baecke and Bocca's (2017) shows that predictive models based on such IoT data sources are already able to assess the accident risk better than traditional models. Additionally, Ingenie (2017) found a direct link between the number of times a driver checks their online feedback with a lower risk of crashing.

Insurer-client relationship

Personalised and augmented service-based offers create a different value relationship with customers. It transforms insurers to supporters of clients who can receive incentives and targets that encourage better behaviour (Scardovi, 2017).

This dynamic may be particularly useful in the health and life insurance sector, where insurers can specify healthy behaviours that will allow for the pricing to be adjusted accordingly. In areas of the market with low margins and high operation costs, this capacity to more accurately charge could provide a real competitive edge.

Gamification

Additionally, IoT opens up opportunities for the gamification of processes in the insurance domain. The latter is also a result of the spread of social media and smartphone apps. Gamification or rather the application of game-design elements and game principles in non-game contexts, may be used to boost customer engagement and can make processes more effective.

Gamified experiences can encourage the alteration of policyholders through, for instance, the incentivisation to achieve certain thresholds such as daily steps. This can be complemented through reward system that can include monetary compensations as well as small gifts such as vouchers for particular services (Leight, 2012).

A.T. Kearney (2014) highlights how there is considerable room for new software development in the insurance sector which may be a way to engage younger consumers by providing them with IoT systems such as wearable devices or Internet-supported home appliances.

Box 16: Insurance for SME's in the IoT environment

Given its wide application across several industry sectors and market segments, the IoT is opening up new opportunities for small business innovation. At the moment, the majority of small and medium size businesses (SMEs) are attracted to the IoT for two main reasons:

1. innovating at the edge, by embedding sensing and connectivity into their existing products (e.g. connected toys); and
2. innovating in services, by providing personalised services based on data analytics gathered by the increased adoption of connected products (e.g. energy trading).

However, IoT SMEs are also facing several challenges, including the difficulty to navigate a fragmented standards landscape as well as challenges internalising cybersecurity best practises into their business model.

In this context, the insurance sector can provide support for SMEs by signalling current practices through their policies, while ensuring that SMEs are both sufficiently encouraged and protected to pursue an innovation pathway.

In this regard, IoT and cyber solutions for SMEs may represent an area for growth for the Lloyd's market.

Platform-based business models and collaborations

The above-mentioned changes will go hand in hand with a shift towards platform-based business models that require strategic partnerships with technology vendors.

Many of these currently act as data 'gatekeepers' but should be brought much closer in order to support innovation and development in insurance products and services.

- Firstly, IoT will drive a growth in collaboration that challenges one-time, static data capture, allowing third parties to offer relevant value to end customers based on their data profiles.

  This could range from discounts for the leasing of systems such as cars to special offers such as the training of staff members based on the information collected by IoT devices.

- Secondly, insurers may also partner with technology vendors and cybersecurity firms to standardise digital assets used by those insured.

  Such engagements may be based on prior agreed criteria (e.g., particular certification programmes) or prior agreed providers (e.g., determined third-party providers).

Both options ensure greater consistency across the client base, but may also risk increased attack vectors should the security of any of these vendors be breached.

Box 17: Citizens engagement platforms

Citizen engagement platforms that use a city mobile app to help users discover and engage with their local area are being developed and tested in cities around the world. The idea is that, instead of citizens using multiple apps to access local amenities, everything is in one place for them.

For example, Loqiva is a mobile city services platform and payments solution where citizens, local businesses and the council can work better together, supported by contextual intelligence and IoT. Citizens experiences like personalised digital advertising displays, sensor-led parking and responsive street lighting can be triggered through the platform using a citizen's mobile phone.

Risks

A smart city vision is to have all IoT devices - from streetlights to building sensors - connected through a single, consolidated network so that councils can manage their resources more effectively. The issue is that every IoT device is a possible point of attack.

Technology can be used to mitigate this risk (e.g. via subnets, Web Application Firewalls, improved IoT firmware, etc.), but the scale and complexity of city-sized systems mean that catastrophic scenarios are, however remote, a possibility. Such scenarios might include a DDoS attack from a group of compromised IoT devices, or a targeted attack on public digital displays or traffic management systems.

Opportunities for commercial insurance

Cities embarking on IoT initiatives are aware of such risks and require technology vendors to manage them. Contractual limitations of liability however, are likely to vary considerably between vendors and cities' IoT projects and potential physical impacts on critical infrastructures might cause significant disruptions. This is where insurers can play a significant role in mitigating the losses of a smart city.

Insurers are well-placed to take advantage of the new wealth of data produced by smart cities. Future-thinking incumbents and insurtechs could help cities, through PPP models, to monetise this data and fund IoT infrastructure. For example, the largest Chinese Insurance company, Ping An is investing more than US$1bn in technology R&D this year. In August, it unveiled their 1+N Smart City Platform at the Fourth China Smart City International Expo in Shenzhen. The platform supports 10 core smart city sectors including: smart administration, insurance, security, transportation, port, financial trade, finance, education, healthcare, real estate, environmental protection, and elderly care.

IoT offers insurers the potential to monitor risk profiles in real-time, enter new markets and deliver services in completely new ways. It is going to be an incredibly disruptive force and, in some market sectors, insurers may need to stay a step ahead and engage with data owners like city councils to stay relevant.

When it comes to monetisation and standards, questions around data ownership, security and privacy arise. Forward thinking councils are looking to hand back data ownership and management to citizens. Many councils also have open data initiatives that allow third parties to freely use and redistribute publicly accessible city data.

Engagement

Today, many IoT projects are moving beyond small-scale pilots towards full-scale city deployments. Insurers may want to get involved into earlier demonstrator projects. To learn more, insurers can engage with cities, industry associations, management consultancies, technology vendors, and smart city consortia. In the UK, the government backed Future Cities Catapult would be the first point of contact for insurers looking to collaborate on new urban technologies like IoT.

A practical solution would be for cities to provide an API to insurers to be able to access authorised datasets. The API would use an agreed IoT data standard for insurance, and insurers would be charged an amount by cities each time a request for data is made. The industry could then take this one step further and aggregate all UK cities data into a single exchange.

5.2 Underwriting

The IoT has the potential to significantly change the underwriting and pricing models of insurance companies (Scardovi, 2017).

By knowing more about their customers and assets, insurers can react to risks in a dynamic way. Thus, the sector is expected by some, to move away from a reactive passivity to a proactive force that mitigates and even prevents claims (Scardovi, 2017).

Methods of calculating losses based on years of historic data may thereby also transform and shift towards the increasing reliance on sophisticated data science and predictive techniques.

Advances in technology mean the sector will reach a point where proxies currently used may no longer be useful or even necessary to understand an individual's behaviour and product usage (McCluskey, 2016).

This means that insurers will be in a better position to assess risk, understand complex exposure (and manage it), as well as estimate the necessary capital reserves, making capital calibration more fluid (EY, 2016).

New product portfolios

Due to the cyber-physical nature of insured assets new product portfolios will emerge. Physical risks are increasingly entangled with cybersecurity concerns, raising the question whether cyber exclusion policies or non-affirmative cyber risks can continue to be upheld.

The "cyber" element of IoT will have to become incorporated in existing products, resulting in changes to virtually all product portfolios. Equally, "cyber" will have to be understood and articulated in a much more granular way than it currently is. Risk codes might too broad to capture the complexities of global IoT supply chains and data flows – particularly in incidental or non-affirmative risk scenarios (Interviewee 3, 26.06.2018).

Further, the systemic exposure of IoT across different insurance line boundaries and the lack of clarity with regards to attribution (and therefore customer service issues; see Section 3) will be a specific challenge to multiple product lines.

For example, property lines where modelling and systemic considerations are arguably more readily available may be better positioned to engage with the challenges that IoT's risk aggregation brings. Whereas, the product recall space and cyber lines, as well as domestic insurances may require more significant reconfiguration.

Box 18: Lloyd's Lab – Parsyl

Parsyl is one of the 10 companies participating in the first cohort of the Lloyd's Lab inaugurated in September 2018.

Parsyl offers an IoT quality assurance and risk management solution that helps insurers and their assured customers understand the quality conditions of sensitive and perishable products as they move through the supply chain, both in transit and storage, from source to final destination. Parsyl's solution is scalable and it offers reliable, objective data on supply chain conditions, allowing users to anticipate supply chain risks in a new way.

The Parsyl platform includes its low cost, proprietary Trek multi-sensing hardware devices (tracking temperature, light, humidity, shock and GPS), mobile application and a web platform that combines granular sensor readings with contextual data, such as cargo tracking, weather and telematics. Parsyl's software automatically generates interactive shipment visualisations, aggregated performance insights and recommendations for avoiding issues with future shipments such as temperature excursions or moisture damage.

Parsyl leverages IoT technology to collect an entirely new primary data set and builds predictive data and analytics on top of it. Using machine learning algorithms, Parsyl allows insurers and their assureds to learn from both "good" and "bad" shipments, getting smarter over time by understanding how different variables impact a shipment outcome and gain deeper oversight of higher accounts.

Parsyl's predictive analytics also allow insurers to improve future risk selection and lower loss adjustment expenses by understanding quality performance patterns over time. And customer claims experiences are greatly enhanced because both insurers and their assureds have access to a single, reliable and shareable source of the truth.

Parsyl is a solution designed to be affordable enough to use in every shipmen with a simple reverse logistics program for returning or reusing Trek devices.

Policy wordings and questionnaires

In a recent study, ENISA (2017b) encouraged the use of standardised policy language and underwriting questionnaires for cyber risk insurance. This is of continuing relevance as insurance covers adapt to the increasingly interdependent ecosystem of the IoT.

In particular, the assessment of risks in interconnected systems could be improved by including questions about the information technology, management, and compliance of a potential policy holder.

Exploring options for data gathering will be important so as to ensure that underwriters comprehensively understand the scale and scope of risks that the IoT creates and the amount and type an customer holds (Romanosky, Ablon, Kuehn, & Jones, 2017).

The standardisation of policy language and questionnaires could also be fostered by the increasing application of machine learning and AI systems, which allows for a more accurate review of policies by actuaries.

Box 19: Policy language and questionnaires

Romanosky et al. (2017) analysed 44 security application questionnaires across over 100 cyber insurance policies filed with US state insurance commissioners.

The authors identified relevant gaps in the used security questionnaires, including missing information about the security posture of third-party services and supply chain providers.

Similarly, questions on the technical infrastructure and businesses interdependencies with the broader technological environment were absent. There was no explicit calling out of mobile devices or systems like drones and other IoT systems.

As these questionnaires are used by carriers to solicit a comprehensive understanding of an applicant's risk profile, it will be important that security measures are becoming more adaptive in the advent of IoT as well as embedded into larger developments such as certification schemes.

5.3 Claims

The IoT is likely to drive further evolution in claims, as the sector begins to orient itself more towards active loss prevention. This will be driven by advances in safety technologies which will impact accident frequency and, thus, premiums (A.T. Kearney, 2014). Besides, IoT has the potential to facilitate the response to fraudulent claims and tackles expensive and long claims processes.

5.4 Capital reserving

Capital reserving will also be affected by the emergence of IoT risks, with capital calibration potentially becoming more fluid. Insurers will have to hold enough reserves to deal with the systemic risks that IoT will generate and amend capital and internal models accordingly.

Challenges

– Understanding the exposure. In some respects, IoT claims may not be all that different to claims previously seen by the sector (Serafin, 2018). However, it is expected that the nature of insurable risks will shift to low-frequency, high-severity events that are harder to predict and price (A.T. Kearney, 2014).

  Understanding the extent of exposure to these events will be critical to ensure that business models are fit for purpose in the IoT with adequate capital reserves in place.

– Homogeneity of risks across the customer base. IoT has the potential to create homogeneity of assets and consequent homogenous risks across insurers' customer base. While in other areas of insurance, such as earthquake or flood coverage, carriers make sure to diversify their customer base, the same spreading of risks connected with the IoT is not possible as has already been observed in the context of cyber risk insurance.

  As similar IoT technologies and vendors are popular across different geographic locations, sectors, and policy holder groups, insurers and especially re-insurers may be subject to an overwhelming number of simultaneous claims (Wolff, 2018). Vulnerabilities such as WannaCry or the Spectre and Meltdown security flaws of Intel chips are examples of this.

  These incidents did not stop at a particular sector and location. In future, through IoT interconnected systems, similar vulnerabilities will exacerbate exposure as chips and software are embedded in previously unconnected devices and systems.

– Near accidents and near misses. To fully understand IoT's opportunities and risks, data on near accidents and near misses could help generate a comprehensive dataset to model risks more effectively. In 2017, Lloyd's explored the benefits of counterfactual risk analysis and proposed a framework to asses near misses that could be used to explore IoT accidents (Lloyd's and Risk Management Solutions., 2017).

5.5 Modelling and exposure management

IoT will have a profound impact on risk modelling. In particular, by combining different data sets, including historical as well as real-time IoT data, insurers will be able to enhance their modelling capabilities.

This will be of significant importance, as IoT – more so than traditional cybersecurity risks – opens up opportunities for the aggregation of risk. While an extreme cyber-attack could cause US$53.1bn (US$121.4 billion - US$15.6 billion 95%confidence interval) in economic losses (Lloyd's & Cyence, 2017), IoT risks are yet to be modelled and assessed.

Nuanced cyber class models

IoT at the moment is not considered as part of the cyber risk modelling process (Interviewee 3, 28.06.2018). There is only one cyber class model which is skewed towards extreme events.

As IoT risks and opportunities emerge, more sophisticated and nuanced cyber class models may need to be developed which account for direct and incidental cyber risks as well as operational risks deriving from the use of emerging technologies. The modelling should also not happen in silos, but rather account for the dependencies and correlations that cyber risks create across different sectors.

Blend and capture

To ensure better IoT modelling, ENISA (2017b) recently recommended the use of high risk use cases such as IoT which may be drawn from the scenarios outlined in this report. ENISA also proposed an industry-wide approach to emerging cybersecurity risks which could support better assessment and a harmonised view of the potential aggregated risks which the IoT will generate.

This requires a blending of cyber ratings with physical asset models. Both risk assessments are currently rather segmented, but will soon face systemic as well as cascading disruptions. In addition, IoT data capture and storage will need to become harmonised and supported by a legal framework that clarifies what kinds of data can be used in order to promote the ethical collection and processing of data.

Box 20: IoT sensors on cargo and Lloyd’s

Lloyd’s (2017a) identified the challenges in accurately pricing cargo insurance in its Market Insight Report *“Goods to go: New approaches to cargo risk modelling”.* Risk models struggle to model factors such as seasonality, logistic path variations, packaging, and regional risks.

Keen to take this concern further, Lloyd’s Data team within the Data Lab engaged Zuhlke Engineering, a software and hardware development consultancy with expertise in the IoT. A mutual hypothesis was proposed: using sensor devices to track cargo flows on a regular basis would provide insight on cargo journeys which would lead to better, more informed risk modelling. It was clear that it was not feasible to track the movement of every piece of cargo, rather selected items on logistics paths of interest.

The first step in testing this hypothesis was for Lloyd’s Data Lab and Zuhlke to engage with the market to gauge their view on the value of data sampled from a variety of typical cargo movements. Workshops were undertaken with a number of insurers, to share with them what was possible in cargo tracking, understand their risk modelling processes, and look for value in combining the two.

With respect to the technology available, cost-effective sensors are available to measure a wide range of factors. Location, temperature, humidity, shocks, vibration, moisture, and light levels all proved to be of interest to the insurers. There are also a number of different approaches to accessing the collected data, from real-time trackers connected via wireless networks to data logger devices.

While insurers deemed that real-time tracker data might be useful for claims processes, either to track high-value shipments or to get live data on unfolding catastrophic events, from a risk-modelling perspective the accuracy and coverage of the data was considered more important than receiving it in real-time.

The hypothesis was well received by the insurers. When examined in detail Lloyd’s, Zuhlke, and the insurance market all agreed that a sampled cargo monitoring initiative would better inform the risk modelling processes. Much risk modelling is driven on qualitative assessments, where relative risks are considered based on agents’ experience of historical claims, knowledge of the logistics network, the perceived vulnerability of specific cargo types and shipping methods, and surveyors’ involvement. Patterns identified from the tracking data are seen as a valuable way to add quantitative insight to a qualitative process.

The actions taken based on these insights could include a more accurate risk model which would highlight to an insurer which business would be expected to be profitable, and which should be avoided. The enhanced model could also influence renewal pricing. Discussing identified risks with customers and capturing these in contract clauses promotes the avoidance of risky shipping practices.

Overall, the Lloyd’s market is very interested in understanding better the story of the voyage. Hence the hypothesis holds value and is worthy of being tested in practice. The next step, which is currently in progress, is to conduct a short trial tracking of a small number of cargo types and routes. If this proves to generate actionable insight, then cargo risk modelling could become yet another area where the IoT brings real business value.

Conclusions

6. Conclusions

Any large-scale technological shift raises challenges to the status quo and creates opportunities for those who see them early on in periods of transformation.

Early adopters, especially in markets, are afforded additional benefits as they are able to shape expectations, terms of engagement, and best practice in ways that address their interests.

While it is never possible to accurately predict how rapidly changing technology will be adopted and implemented, giving careful consideration to possible future scenarios allows us to systematically think through what form those challenges and opportunities might take and how to make IoT benefit the greater good.

Based on our research, we present five key findings for insurers. These findings are interconnected and thus require a holistic approach to the IoT technological transformation.

Key findings

1. The IoT will lead to data capture and management at unprecedented scale. Increasingly traceable, granular data streams will provide input to enhanced risk diagnostics and real-time, bespoke and flexible products. Concerns for policy holders regarding the privacy and representative accuracy of data capture need to be addressed.
2. New types of threats and harms will emerge, such as the use of IoT devices as attack vectors and long-term resultant socio-economic impacts on individuals and organisations. This will necessitate innovation in both existing and new lines of business.
3. The scale and variability of disruption will expand and cascade across sectors and lines of business. The influence of legacy systems with variable security standards poses a critical uncertainty for future risk assessment
4. Insurance policies will increasingly influence and manage risks behaviour. Personalisation of policies will be capable of predicting and mitigating risk based on large scale data and trends analysis.
5. There are critical blind spots in the regulation and legislation of IoT devices and their impacts. These include uncertainties surrounding attribution and liability concerning algorithmic bias and software design.

New business models

Business models for writing insurance and the operational dimension of the sector will change and those who lead this change will set the agenda for others who follow.

A combination of data, automation, and human innovation will be required to develop the value proposition for the IoT. We do not yet have the necessary methodologies to estimate the value added from IoT implementations or the risk of loss.

Adapting to the IoT will necessitate reshaping the workforce in the insurance sector so that opportunities can be fully exploited. As one interviewee expressed, *“spreadsheets are no longer fit for purpose – actuaries need programming skills instead”* (Interviewee 5, 10.07.2018).

Automation in the underwriting process and in optimising pricing will introduce new efficiencies. Distinguishing between those roles that will be automated and those that cannot be removed from human oversight will allow for the timely recalibration of skills and human resources.

Once these practices are more mature, insurance as a service will replace insurance as a product. When this happens, reducing the many layers between the customer and the capacity provider will allow for large scale capture of very small margins. In this context, IoT and cyber solutions for SMEs may represent an area for growth for the Lloyd’s market.

IoT data, scenarios analysis and risk modelling

The exponential growth of data that will come about as a consequence of IoT implementations will allow for much more sophisticated, granular and accurate scenarios analysis and risk modelling.

Currently, 'cyber' is a broad concept in insurance and it will need to be broken down into much greater detail to be effective in modelling risk and exposure, shaping coverage and guiding capital reserve requirements. As a start to help quantify the impact of IoT events this paper provides ten scenarios in four sectors: water, agriculture, maritime, and the home.

In order to redress the exponential growth of data, a much closer partnership with the tech sector is necessary. Expertise and cutting-edge developments in data science could be integrated into the insurance sector through collaborative relationships.

Finding ways to capture useful data, developing the business infrastructure to manage and use that data and turning it into effective and dynamic risk models will be fundamental to the future of insurance in the IoT.

This presents real opportunities of scale and can be adopted from sectors that already excel in it. Another important reason for bringing the insurance sector into closer contact with the tech sector is to maximise that market.

When insuring businesses at the cutting edge of emerging technology which, themselves, are exploring new business models, it is important that those in the insurance sector have adequate support to understand and interpret their risk.

Where the IoT is so close to individuals, sometimes in life critical systems like cars or healthcare, there is significant potential for better understanding and quantifying risky behaviour that should or could impact on pricing.

Again, this suggests more personalised, granular and above all, dynamic cover that can rapidly adjust to constantly changing risk landscapes. There is also however, potential down this path for psychological injuries, including in minors who are exposed to damaging or harmful situations.

Aggregated systemic risk

The IoT relies upon global supply chains of components, devices, services, and data flows. Vulnerabilities in any of these could be exploited through wide-ranging systems and implementations, some seemingly unrelated.

This added complexity and new interdependencies will generate layers of 'nested liability' that could be very difficult to assign. Aggregated systemic risk will be less predictable in the IoT and also more probable.

Leadership and governance through the insurance sector

The insurance sector will not only be called upon to respond to the IoT in the ways outlined above. It is expected that it will shape the IoT through a combination of leadership and governance by regulating how coverage is conceptualised, how it is written and what expectations surround liability and risk management.

In order to do this purposefully, a number of opportunities should be considered.

1. Insurers can play a powerful role in the standardisation of data, with data capture and integration having already been emphasised by the London Market Group's Target Operating Model[w] (LM TOM, 2018a, 2018b). The standardisation of data will be central to effective data capture and the consequent potential for large scale data analysis. Lloyd's has the power to drive baseline requirements on which data is captured and how it is handled and shared.

   This could fundamentally improve the whole market, making the modelling of risk and the product portfolios more competitive. There is currently some scepticism in the sector that the vast amounts of data that will be continuously generated through the IoT will ever be able to be captured and translated into useful application. This scepticism is based on the extent to which people already feel overwhelmed by information, not the limits of data science and automation.

   The Lloyd's Lab will be central to this, liaising between different stakeholders to assess their needs and interpret them through innovative applications (in partnerships with InsurTech and technology companies).

[w] There are existing Cyber Exposure Data standards and schemas (see: Lloyd's, 2016; AIR Worldwide, 2016 and Cambridge Centre for Risk Studies, 2016).

2. As the IoT evolves and the insurance sector matures within it, it should take a proactive role in talk to insureds and potential clients to review and assess all risks rather than just the insurable risks associated with IoT.

   By taking a leadership role in this space the insurance sector will acquire the body of knowledge necessary to provide insureds with guidance on IoT best practices, thereby shaping the ecosystem in which they operate.

3. The insurance sector will be directly affected by these changes, not only when referring to IoT security and safety guidelines in their policy design, but also in promoting best practice in key industry sectors where IoT risks are emerging, such as transport, utilities and industrial processes.

   By working closely with governments, regulators, and technology companies, the insurance sector can play a key role in making the IoT more secure, reshaping business models, opening up new markets and scope for innovation, and contributing to the global technological transformation that holds so much potential for improving the human condition.

To conclude, any large-scale technological shift raises challenges to the status quo and opportunities for those who see them. Early adopters, especially in markets, are afforded additional benefits as they are able to shape expectations, terms of engagement and best practice in ways that address their own interests.

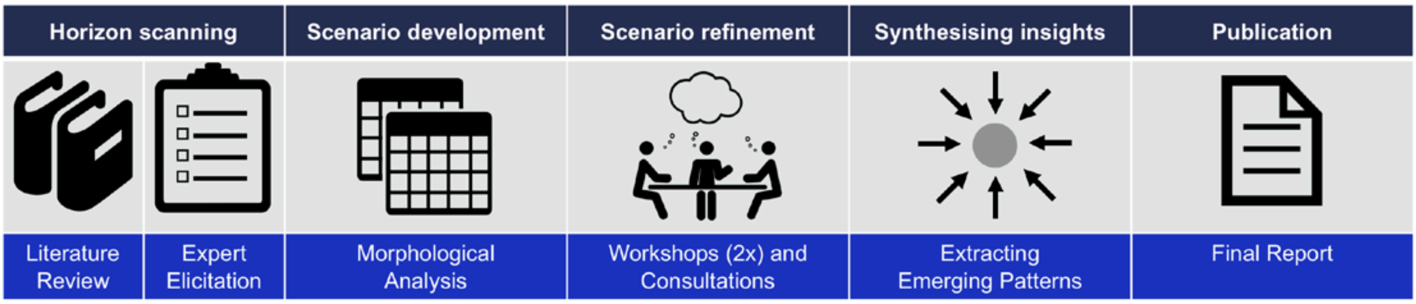
While it is never possible to accurately predict how rapidly changing technology will be adopted and implemented, considering possibly future scenarios allow us to systematically think through what form those challenges and opportunities might take.

In order to do this, it is important to recognise that the IoT is not just *more* technology but that there are some fundamental differences that warrant close attention from the insurance sector.

Appendix: Research approach

This report was developed through a structured research process, across five stages. Each stage was primarily informed by a particular subset of data collection and analysis activities which are summarised in Figure 1 *(below)*.

Figure 1: Research stages



Source: UCL, 2018

Horizon scanning

In order to identify key trends and drivers shaping emerging risks in the IoT, this research commenced with an analytic process frequently used to explore the systemic impacts of emerging technologies: “scanning the future horizon”.

Such scanning exercises seek to identify early signals of emerging issues, trends, or drivers of change; compile these, and then analyse them for their likely significance (Amanatidou et al., 2012; van Rij, 2010).

Two data sources were used as input for the horizon scanning phase: first, academic and expert community literature and second, expert elicitation.

Literature review

The literature reviewed focused on identifying and collating global research and evidence relating to IoT risks and macro-level trends and drivers of change that may impact risk trajectories.

Data sources included media outlets, academic publications, and practitioner literature. 141 UK news magazine stretching from 2003-2018 (n=960; cut-off date 15th of January) were reviewed.

The research team drew also on existing research projects taking place within the PETRAS IoT Research Hub. This background research helped to identify:

- Global research and evidence relating to IoT risks;
- Macro-level trends and drivers of change that may impact risk trajectories.

Experts elicitation survey

An expert elicitation survey supported the literature review. The survey focused on identifying and categorising the different types of risks that experts anticipate the IoT will create.

Respondents were drawn primarily from the UK IoT (PETRAS) community, other industry experts operating within the wider IoT and cybersecurity field, and technology disruption analysis experts (*n=24*).

A snowball sampling method, which is a non-probability sampling technique that allowed respondents to suggest additional individuals or organisations to contribute to the research was applied (Biernacki & Waldorf, 1981).

The expert elicitation survey helped to:

- Identify and categorise the different types of risks that the experts anticipate the IoT will create;
- Engage a wider community of subject experts; and
- Triangulate results.

Scenarios development

In examining the potential impacts of emergent technologies, interactions between different trends and drivers of change were explored.

The evaluation of such causal interactions is typically undertaken using 'scenarios', which are coherent stories that describe how the world might look in the future when multiple critical uncertainties combine.

Morphological analysis

Morphological analysis is a technique to systematically identify future scenarios from a total set of multiple thousands of possible future combinations (Ritchey, 2011).

The inputs for this analysis take the key insights from the literature review and the horizon scanning exercise and combined them with an identified list of possible impact areas of interest.

The resultant output is a table that offers a "menu of options", which facilitated the initial scenario development. Common drivers of change, threats, and risks were considered and relevant sectors and contexts for further in-depth examination determined. Prioritisation and selection of scenarios and sectors was undertaken in consultation with Lloyd's.

Scenarios refinement

Workshops and consultation with subject experts and underwriters

Following this initial scoping and scenario development, Lloyd's together with STEaPP and PETRAS conducted one collaborative workshop sessions that involved underwriters and subject specialist across prior agreed sectors as well as a one with cybersecurity specialists at the Academic Centres of Excellence for Cybersecurity Research (ACE-CSR) conference. In-depth semi-structured interviews (*n=5*) with underwriters and actuaries supported the consultation process.

The purpose of these workshops and interviews was to share initial research findings and to stress-test the scenarios that derived from the horizon scanning and morphological analysis.

The subject experts and underwriters offered practical criticism and feedback on the applicability, likelihood, and relevance of the scenarios and highlighted potential implications and considerations for the insurance industry. The insights derived from these workshops and interviews were used to amend and improve the scenarios in consultation with Lloyd's.

Following this systematic collection and development of scenarios, ten scenarios were selected for final elaboration. The scenarios were selected due to their relevance for the insurance sector and forward-thinking outlook on emerging risks in the IoT. These scenarios form the basis of the detailed analysis provided in Section 6 of this report.

Research approach outcomes

The here discussed scenarios point to an emerging and changing risk landscape. Lloyd's, STEaPP, and PETRAS hope this study adds to the knowledge base, stimulates new ideas, and raises new research questions and projects.

The findings will deepen insurers' and risk managers' understanding of the evolving IoT ecosystem and reveal how the IoT may interconnect with established and emerging insurance products such as cyber risk insurance.

Continued research, reflection and collaboration across sectors and industries will be critical to address some of the anticipated constraints and problems of the IoT and can support the development of a more resilient, inclusive, prosperous cyber-physical infrastructure.

References

Adapa, A., Nah, F. F.-H., Hall, R. H., Siau, K., & Smith, S. N. 2017. Factors Influencing the Adoption of Smart Wearable Devices. International Journal of Human–Computer Interaction, 0(0), 1–11. https://doi.org/10.1080/10447318.2017.1357902

AIOTI WG04. 2015. AIOTI Working Group 4 – Policy. Brussels: Alliance for Internet of Things Innovation. Retrieved from https://aioti.eu/wp-content/uploads/2017/03/AIOTIWG04Report2015-Policy-Issues.pdf

AIR Worldwide. 2016. AIR Cyber Exposure Data Schema and Preparer’s Guide. Retrieved August 30, 2018, from http://www.air-worldwide.com/Documentation/Cyber-Exposure-Data-Standard/air_cyber_exposure_data_schema_and_preparers__guide.htm

Allianz. 2017. Safety considerations and regulation key to progress of autonomous vessels. Retrieved May 6, 2018, from http://www.agcs.allianz.com/insights/expert-risk-articles/safety-shipping-2017-autonomous-shipping/

Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. 2017. Fog Computing for the Internet of Things: Security and Privacy Issues. IEEE Internet Computing, 21(2), 34–42. https://doi.org/10.1109/MIC.2017.37

alva. 2018. Cybersecurity and the risk to reputation. An analysis of recent security breaches - TalkTalk (pp. 1–12). London, New York: alva. Retrieved from http://www.alva-group.com/en/case-study/report-cybersecurity-risks-reputation/

Amanatidou, E., Butter, M., Carabias, V., Könnölä, T., Leis, M., Saritas, O., … van Rij, V. 2012. On concepts and methods in horizon scanning: Lessons from initiating policy dialogues on emerging issues. Science and Public Policy, 39(2), 208–221. https://doi.org/10.1093/scipol/scs017

Anderson, E. L., Steen, E., & Stavropoulos, V. 2017. Internet use and Problematic Internet Use: a systematic review of longitudinal research trends in adolescence and emergent adulthood. International Journal of Adolescence and Youth, 22(4), 430–454. https://doi.org/10.1080/02673843.2016.1227716

Aon. 2017. Global Cyber Market Overview. Uncovering the Hidden Opportunities (p. 16). London: Aon Inpoint. Retrieved from http://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf

Apthorpe, N., Reisman, D., Sundaresan, S., Narayanan, A., & Feamster, N. 2017. Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic. ArXiv:1708.05044 [Cs]. Retrieved from http://arxiv.org/abs/1708.05044

Assem, H., Xu, L., Buda, T. S., & O’Sullivan, D. 2016. Machine learning as a service for enabling Internet of Things and People. Personal and Ubiquitous Computing, 20(6), 899–914. https://doi.org/10.1007/s00779-016-0963-3

A.T. Kearney. 2014. The Internet of Things: Opportunity for Insurers (pp. 1–10). Chicago: A.T. Kearney Limited. Retrieved from https://www.atkearney.co.uk/documents/10192/5320720/Internet+of+Things+-+Opportunity+for+Insurers.pdf/4654e400-958a-40d5-bb65-1cc7ae64bc72

Banham, R. 2017. Investing in the Insurtech Toolbox. Risk Management; New York, 64(6), 12–14.

Barthelsson, P., & Sagefjord, J. 2017. Autonomous ships and the operator’s role in a Shore Control Centre - A comparative analysis on projects in the Scandinavian region and implementing the experience of Mariners to a new field of shipping (Master Thesis). Chalmers University of Technology, Gothenburg, Sweden. Retrieved from http://studentarbeten.chalmers.se

Bateman, T. 2013, October 16. Police warn over drugs cyber-attack. BBC News. Retrieved from http://www.bbc.co.uk/news/world-europe-24539417

Bauer, H., Burkacky, O., & Knochenhauer, C. 2017, May. Security in the Internet of Things [McKinsey & Company]. Retrieved June 18, 2018, from https://www.mckinsey.com/industries/semiconductors/our-insights/security-in-the-internet-of-things

Bayer. 2018. The Future of Agriculture and Food. Facts and figures (pp. 1–30). Leverkusen: Bayer AG. Retrieved from https://www.bayer.com/en/bay-landwirtschaft-ernaehrung-fakten-en-final.pdfx?forced=true

Bedi, G., Venayagamoorthy, G. K., Singh, R., Brooks, R. R., & Wang, K. C. 2018. Review of Internet of Things (IoT) in Electric Power and Energy Systems. IEEE Internet of Things Journal, 5(2), 847–870. https://doi.org/10.1109/JIOT.2018.2802704

Bertolino, A., Calabro', A., Giandomenico, F. D., Lami, G., Lonetti, F., Marchetti, E., … Mori, P. 2017. A tour of secure software engineering solutions for connected vehicles. Software Quality Journal, 1–34. https://doi.org/10.1007/s11219-017-9393-3

BEUC. 2017. Review of Product Liability Rules (pp. 1–11). Brussels: European Consumer Organisation. Retrieved from http://www.beuc.eu/publications/beuc-x-2017-039_csc_review_of_product_liability_rules.pdf

Biernacki, P., & Waldorf, D. 1981. Snowball sampling: Problems and techniques of chain referral sampling. Sociological Methods & Research, 10(2), 141–163.

Binu, P. K., Akhil, V., & Mohan, V. 2017. Smart and secure IoT based child behaviour and health monitoring system using hadoop. In 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 418–423). https://doi.org/10.1109/ICACCI.2017.8125876

Bitton, G. 2014. Bioterrorism and Drinking Water Safety. In G. Bitton (Ed.), Microbiology of Drinking Water (pp. 153–171). Hoboken, New Jersey: Wiley-Blackwell. https://doi.org/10.1002/9781118743942.ch7

Blythe, J., & Lefevre, C. 2018. Cyberhygiene Insight Report (pp. 1–12). London: IoTUK and PETRAS IoT Hub. Retrieved from https://iotuk.org.uk/wp-content/uploads/2018/01/PETRAS-IoTUK-Cyberhygiene-Insight-Report.pdf

Boothby, W. H. 2014. The Legal Challenges of New Technologies: An Overview. In New Technologies and the Law of Armed Conflict (pp. 21–28). The Hague: T.M.C. Asser Press. https://doi.org/10.1007/978-90-6704-933-7_2

Brass, I. 2018. Standardising IoT Security: Implications for Digital Forensics. Digital Forensics Magazine, (53), 44–49. https://www.petrashub.org/wp-content/uploads/2018/07/BRA001-pdf.pdf

Brass, I., Carr, M., Tanczer, L., Maple, C., & Blackstock, J. 2017. Unbundling the Emerging Cyber-Physical Risks in Connected and Autonomous Vehicles (Connected and Autonomous Vehicles: The emerging legal challenges) (pp. 8–9). London: Pinsent Masons. Retrieved from https://www.pinsentmasons.com/PDF/2017/Freedom-to-Succeed-AMT/Connected-autonomous-vehicles-report-2017.pdf

Brass, I., Tanczer, L., Carr, M., Elsden, M., & Blackstock, J. 2018. Standardising a Moving Target: The Development and Evolution of IoT Security Standards. In Living in the Internet of Things: Cybersecurity of the IoT - 2018. London, UK: IET. https://doi.org/10.1049/cp.2018.0024

Braun, A., & Schreiber, F. 2017. The Current InsurTech Landscape: Business Models and Disruptive Potential. St. Gallen: Institute of Insurance Economics IVW-HSG. Retrieved from https://www.ivw.unisg.ch/_/media/internet/content/dateien/instituteundcenters/ivw/studien/ab-insurtech_2017.pdf

Brazilian Development Bank, Ministry of Planning, Budget, and Management, & Ministry of Science, Technology, Innovation and Communication. 2017. Internet of Things: An Action Plan for Brazil (pp. 1–26). Brasília: Government of Brazil. Retrieved from http://www.funag.gov.br/images/2017/Novembro/Dialogos/Claudio_Leal-Internet-of-Things.pdf

Buchmann, J., Lauter, K., & Mosca, M. 2017. Postquantum Cryptography #x2014;State of the Art. IEEE Security Privacy, 15(4), 12–13. https://doi.org/10.1109/MSP.2017.3151326

BusinessEurope. 2016. Liability for defective products – public consultation (pp. 1–5). Brussels: Confederation of European Business. Retrieved from https://www.businesseurope.eu/sites/buseur/files/media/position_papers/legal/2017-04-26_product_liability_-_reply_to_consultation.pdf

Cambridge Centre for Risk Studies. 2015. Cyber Exposure Data Schema. University of Cambridge Judge Business School: Centre for Risk Studies; Retrieved from https://www.jbs.cam.ac.uk/faculty-research/centres/centre-for-risk-studies/publications/space-and-technology/cyber-exposure-data-schema/

Cam-Winget, N., Sadeghi, A. R., & Jin, Y. 2016. Invited: Can IoT be secured: Emerging challenges in connecting the unconnected. In 2016 53nd ACM/EDAC/IEEE Design Automation Conference (DAC) (pp. 1–6). https://doi.org/10.1145/2897937.2905004

Charara, S. 2018, February 6. What the smart home will look like in 2020, 2040 and beyond. Retrieved August 16, 2018, from https://www.the-ambient.com/features/future-of-smart-home-timeline-310

CISCO. 2015. Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are (pp. 1–6). San Jose, CA: CISCO. Retrieved from https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf

Davis II, J. S., Boudreaux, B., Welburn, J. W., Aguirre, J., Ogletree, C., McGovern, G., & Chase, M. S. 2017. Stateless Attribution. Toward International Accountability in Cyberspace (pp. 1–64). Santa Monica: RAND Corporation. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2081/RAND_RR2081.pdf

Deloitte. 2017. Tech Trends 2017: The Kinetic Enterprise (pp. 1–140). New York: Deloitte University Press. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology/gx-tech-trends-the-kinetic-enterprise.pdf

DeNardis, L., & Raymond, M. 2017. The Internet of Things as a Global Policy Frontier. UC Davis School of Law, 51, 475–487.

Dijk, R. van, Liang, W., Zhang, B., & Hu, J. 2017. Development and Evaluation of a Non-obtrusive Patient Monitoring System with Smart Patient Beds. In Distributed, Ambient and Pervasive Interactions (pp. 482–490). Springer, Cham. https://doi.org/10.1007/978-3-319-58697-7_36

Edmondson, V., Cerny, M., Lim, M., Gledson, B., Lockley, S., & Woodward, J. 2018. A smart sewer asset information model to enable an ‘Internet of Things’ for operational wastewater management. Automation in Construction, 91, 193–205. https://doi.org/10.1016/j.autcon.2018.03.003

EIOPA. 2017. EIOPA InsurTech Roundtable: How technology and data are reshaping the insurance landscape (pp. 1–17). Frankfurt: European Insurance and Occupational Pensions Authority. Retrieved from https://eiopa.europa.eu/Publications/Reports/08.0_EIOPA-BoS17-165_EIOPA_InsurTech_Roundtable_summary.pdf

Ekelhart, A., Neubauer, T., & Fenz, S. 2009. Automated risk and utility management. In Information Technology: New Generations, 2009. ITNG’09. Sixth International Conference on (pp. 393–398). Las Vegas, Nevada: IEEE.

ENISA. 2017a. Baseline Security Recommendations for IoT in the context of Critical Information Infrastructure. Retrieved from https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

ENISA. 2017b. Communality of risk assessment language in cyber insurance. Recommendations on Cyber Insurance (pp. 1–53). Heraklion, Greece: European Union Agency for Network and Information Security. Retrieved from https://www.enisa.europa.eu/publications/commonality-of-risk-assessment-language-in-cyber-insurance

Environmental Agency. 2018, February 16. Climate change means more frequent flooding, warns Environment Agency. Retrieved June 19, 2018, from https://www.gov.uk/government/news/climate-change-means-more-frequent-flooding-warns-environment-agency

European Commission. 2017a. Brief factual summary on the results of the public consultation on the rules on producer liability for damage caused by a defective product (No. GROW/B1/HI/sv(2017) 3054035) (pp. 1–111). Brussels: European Commission. Retrieved from http://ec.europa.eu/docsroom/documents/23471

European Commission. 2017b. Industry 4.0 in agriculture: Focus on IoT aspects (Digital Transformation Monitor) (pp. 1–6). Brussels: European Commission. Retrieved from https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Agriculture%204.0%20IoT%20v1.pdf

European Commission. 2018. SWD(2018) 157 final: Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (pp. 1–108). Brussels: European Commission. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0157&from=en

EY. 2013. The quest for Telematics 4.0 (p. 8). London: Ernst & Young Global Limited. Retrieved from https://webforms.ey.com/Publication/vwLUAssets/The_quest_for_Telematics_4.0/$File/The_quest_for_Telematics_4_0.pdf

EY. 2016. The internet of things in insurance (pp. 1–11). London: Ernst & Young Global Limited. Retrieved from https://webforms.ey.com/Publication/vwLUAssets/EY_-_The_internet_of_things_in_insurance/$FILE/EY-the-internet-of-things-in-insurance.pdf

EZ-Link. 2018. EZ-Link – EZ-Link Rewards with Perx [EZ-Link]. Retrieved August 29, 2018, from https://www.ezlink.com.sg/perx

Feng, S., Setoodeh, P., & Haykin, S. 2017. Smart Home: Cognitive Interactive People-Centric Internet of Things. IEEE Communications Magazine, 55(2), 34–39. https://doi.org/10.1109/MCOM.2017.1600682CM

Floresca, L. 2018, January 5. The Intel Chip Security Flaw: What it Means For Cyber Insurance I Equivity. Retrieved January 11, 2018, from https://wsandco.com/cyber-liability/intel-chip-security-flaw-cyber-insurance/

Forcolin, M., Fracasso, E., Tumanischvili, F., & Lupieri, P. 2011. EURIDICE — IoT applied to logistics using the Intelligent Cargo concept. In 2011 17th International Conference on Concurrent Enterprising (pp. 1–9). Aachen, Germany: IEEE.

Frontier Economics. 2018. The Economic Impact of IoT. Putting numbers on a revolutionary technology (pp. 1–6). Madrid: Frontier Economics. Retrieved from https://www.frontier-economics.com/documents/2018/03/internet-things_march-2018.pdf

Futurezone. 2018, January 14. Niederlande: Erste „Tesla-Schiffe“ ab Herbst unterwegs. Retrieved January 15, 2018, from https://futurezone.at/digital-life/niederlande-erste-tesla-schiffe-ab-herbst-unterwegs/306.486.584

Gaspar, R. de P., Bonacin, R., & Gonçalves, V. P. 2018. Designing IoT Solutions for Elderly Home Care: A Systematic Study of Participatory Design, Personas and Semiotics. In Universal Access in Human-Computer Interaction. Virtual, Augmented, and Intelligent Environments (pp. 226–245). Springer, Cham. https://doi.org/10.1007/978-3-319-92052-8_18

Geetha, S., & Gouthami, S. 2017. Internet of things enabled real time water quality monitoring system. Smart Water, 2, 1. https://doi.org/10.1186/s40713-017-0005-y

GhaffarianHoseini, A., Dahlan, N. D., Berardi, U., GhaffarianHoseini, A., & Makaremi, N. 2013. The essence of future smart houses: From embedding ICT to adapting to sustainability principles. Renewable and Sustainable Energy Reviews, 24, 593–607. https://doi.org/10.1016/j.rser.2013.02.032

Goodling, R. C. J. 2016. Top 5 Dairy States Vary in Production, Feed Cost, and Income over Feed Cost. Retrieved September 19, 2018, from https://extension.psu.edu/top-5-dairy-states-vary-in-production-feed-cost-and-income-over-feed-cost

Government Office for Science. 2017. Foresight future of the sea: industry perspectives on emerging technology. London: Government Office for Science. Retrieved from https://www.gov.uk/government/publications/future-of-the-sea-industry-perspectives-on-emerging-technology

Griffiths, H. 2017. Structure of the UK Automotive Telematics Market. With a focus on the use of telematics in road safety solutions (p. 29). London: IoTUK.

HR Wallingford. 2015. CCRA2: Updated projections for water availability for the UK Final Report (No. MAR5343-RT002-R05- 00) (pp. 1–151). Oxford: HR Wallingford. Retrieved from https://www.theccc.org.uk/wp-content/uploads/2015/09/CCRA-2-Updated-projections-of-water-availability-for-the-UK.pdf

Hristov, K. 2017. Internet plus policy: A study on how China can achieve economic growth through the internet of things. Journal of Science and Technology Policy Management, 8(3), 375–386. https://doi.org/10.1108/JSTPM-03-2017-0007

Hsu, C.-W., & Yeh, C.-C. 2017. Understanding the factors affecting the adoption of the Internet of Things. Technology Analysis & Strategic Management, 29(9), 1089–1102. https://doi.org/10.1080/09537325.2016.1269160

IHS Markit. 2017. The Internet of Things: A movement, not a market (pp. 1–9). Englewood, Colorado, United States: IHS Markit. Retrieved from https://cdn.ihs.com/www/pdf/IoT_ebook.pdf

Industrie 4.0 Working Group. 2013. Securing the future of German manufacturing industry. Recommendations for implementing the strategic initiative INDUSTRIE 4.0. (pp. 1–82). Berlin: Office of the Industry-Science Research Alliance, Federal Ministry of Education and Research. Retrieved from http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Material_fuer_Sonderseiten/Industrie_4.0/Final_report__Industrie_4.0_accessible.pdf

King, A. 2017. Technology: The Future of Agriculture. Nature, 544(7651), 21–23. https://doi.org/10.1038/544S21a

Kretschmann, L., Burmeister, H.-C., & Jahn, C. 2017. Analyzing the economic benefit of unmanned autonomous ships: An exploratory cost-comparison between an autonomous and a conventional bulk carrier. Research in Transportation Business & Management, 25, 76–86. https://doi.org/10.1016/j.rtbm.2017.06.002

Kshetri, N. 2017. Can Blockchain Strengthen the Internet of Things? IT Professional, 19(4), 68–72. https://doi.org/10.1109/MITP.2017.3051335

Leight, S. 2012. Smart insurers turn to gamification as a way to change agent behaviour. Infosys BPO, 7–14.

Liu, J., Xiao, Y., & Chen, C. P. 2012. Authentication and access control in the internet of things. In Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on (pp. 588–592). IEEE.

Lloyd’s. 2015. Food system shock: The insurance impacts of acute disruption to global food supply (Lloyd’s Emerging Risk Report) (pp. 1–30). London: Lloyd’s. Retrieved from https://www.lloyds.com/news-and-risk-insight/risk-reports/library/society-and-security/food-system-shock

Lloyd's. 2016. Cyber Core Data Requirements. Retrieved from: https://www.lloyds.com/market-resources/data-and-research/cyber-core-data-requirements

Lloyd’s. 2017a. Realistic Disaster Scenarios (RDS). London: Lloyd’s. Retrieved from https://www.lloyds.com/market-resources/underwriting/realistic-disaster-scenarios-rds

Lloyd’s and Risk Management Solutions. 2017. Reimagining History: Counterfactual risk analysis (Lloyd’s Emerging Risk Report) (pp. 1–49). London: Lloyd’s. Retrieved from https://www.lloyds.com/news-and-risk-insight/risk-reports/library/understanding-risk/reimagining-history

LLoyd’s & ARUP. 2017. Future Cities: Building Infrastructure Resilience (Lloyd’s Emerging Risk Report) (pp. 1–66). London: Lloyd’s. Retrieved from https://www.lloyds.com/news-and-risk-insight/risk-reports/library/society-and-security/arup

Lloyd’s & Cambridge Centre for Risk Studies. 2015. Business Blackout (Emerging Risks Report) (pp. 1–68). London: Lloyd’s. Retrieved from https://www.lloyds.com/news-and-insight/risk-insight/library/society-and-security/business-blackout

Lloyd’s & Cyence. 2017. Counting the cost: Cyber exposure decoded (Emerging Risks Report) (pp. 1–56). London: Lloyd’s. Retrieved from https://www.lloyds.com/news-and-insight/risk-insight/library/technology/countingthecost

Lloyd’s Register. 2016. Cyber-enabled ships. ShipRight procedure - autonomous ships (pp. 1–30). London: Lloyd’s Register. Retrieved from http://info.lr.org/l/12702/2016-07-07/32rrbk

Lloyd’s & Risk Management Solutions. 2018. Harvesting opportunity. Exploring crop (re)insurance risk in India. (pp. 1–145). London: Lloyd’s. Retrieved from https://www.lloyds.com/news-and-risk-insight/risk-reports/library/society-and-security/harvesting-opportunity

LM TOM. 2018a. Data Integration (DI): Sharing information seamlessly by using the same language. Retrieved August 30, 2018, from https://tomsupports.london/data-integration

LM TOM. 2018b. Structured Data Capture (SDC): A key step towards straight through processing. Retrieved August 30, 2018, from https://tomsupports.london/structured-data-capture

LMA. 2018. Cyber Risks & Exposures Model Clauses: Class of Business Review (pp. 1–45). London: Lloyd’s Market Association.

Loit, F., Sivanathant, A., Gharakheilit, H. H., Radford, A., & Sivaramant, V. 2017. Systematically Evaluating Security and Privacy for Consumer IoT Devices. In IoT S&P 2017 (pp. 1–6). Dallas, Texas: ACM CCS. https://doi.org/10.1145/3139937.3139938

Longe, O., & Ouahada, K. 2018. Mitigating Household Energy Poverty through Energy Expenditure Affordability Algorithm in a Smart Grid. Energies, 11(4), 947. https://doi.org/10.3390/en11040947

Maersk, V.-. 2018, January 16. Maersk and IBM to form joint venture applying blockchain to improve global trade and digitize supply chains. Retrieved May 8, 2018, from http://www.maersk.com/en/press/press-release-archive/maersk-and-ibm-to-form-joint-venture

Marsh, & BRINK. 2017. The Changing Tide of Risk: Expert Perspectives on the Marine Industry (pp. 1–70). New York: Marsh & McLennan Companies' Global Risk Center . Retrieved from https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/Emerging%20Trends%20in%20Shipping.pdf

Matthews, C. 2017, September 4. Unmanned "ghost" ships are coming. Retrieved June 18, 2018, from http://theconversation.com/unmanned-ghost-ships-are-coming-83324

McCluskey, B. 2016. Policy pressure: IoT-based cyber-insurance. Engineering &Technology, 11(9), 28–30. https://doi.org/10.1049/et.2016.0900

Meinhardt, P. L. 2015. Water and Bioterrorism: Preparing for the Potential Threat to U.S. Water Supplies and Public Health. Annual Review of Public Health, 26, 213–237. https://doi.org/10.1146/annurev.publhealth.24.100901.140910

Nordrum, A. 2016, August 18. Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated. Retrieved September 2, 2017, from http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated

Nurse, J. R. C., Creese, S., & Roure, D. D. 2017. Security Risk Assessment in Internet of Things Systems. IT Professional, 19(5), 20–26. https://doi.org/10.1109/MITP.2017.3680959

OECD. 2003. Social Issues in the Provision and Pricing of Water Services. Paris: OECD. Retrieved from https://www.oecd-ilibrary.org/environment/social-issues-in-the-provision-and-pricing-of-water-services_9789264099890-en

OECD. 2007. Infrastructure to 2030: Volume 2 - Mapping Policy for Electricity, Water and Transport (pp. 1–510). Paris: Organisation for Economic Co-operation and Development. Retrieved from https://www.oecd.org/sti/futures/infrastructureto2030/40953164.pdf

OECD. 2017. Supporting an effective cyber insurance market. OECD Report for the G7 Presidency (pp. 1–20). Paris, France: Organisation for Economic Co-operation and Development. Retrieved from https://www.oecd.org/daf/fin/insurance/Supporting-an-effective-cyber-insurance-market.pdf

Perry, A. 2016. Consumers' acceptance of smart virtual closets. Journal of Retailing and Consumer Services, 33, 171–177. https://doi.org/10.1016/j.jretconser.2016.08.018

Pimenta, N., Chaves, P., Fernandes, L., & Freitas, D. 2017. Motion Detection in an Intelligent Textile Mattress Cover. In Ambient Intelligence– Software and Applications – 8th International Symposium on Ambient Intelligence (ISAmI 2017) (pp. 47–54). Springer, Cham. https://doi.org/10.1007/978-3-319-61118-1_7

Public-Private Analytic Exchange Program. 2018. Threats to Precision Agriculture (p. 25). Washington D.C.: Department of Homeland Security. Retrieved from https://www.dhs.gov/sites/default/files/publications/2018%20AEP_Threats_to_Precision_Agriculture.pdf

Puertas, A., O'Driscoll, C., Krusberg, M., Gromek, M., Popovic, P., Teigland, R., … Sundberg, T. 2017. The Next Wave of Fintech. Redefining Financial Services through Technology (pp. 1–40). Stockholm: Stockholm School of Economics. Retrieved from https://www.hhs.se/contentassets/cbe0e571708643418a3f0b7e7a18883f/insurtechregtechsse.pa2017.pdf

PwC. 2017a. Ready for take off. How InsurTech are poised to transform insurance (pp. 1–40). London: Startupbootcamp, PwC. Retrieved from https://www.pwc.co.uk/financial-services/start-up-bootcamp/startupbootcampinsurtech_trends_report_2017_online.pdf

PwC. 2017b. The Future is Coming: Index of Cities Readiness (pp. 1–17). Moscow: PricewaterhouseCoopers. Retrieved from https://www.pwc.ru/ru/assets/the-future-is-coming-eng.pdf

PwC. 2017c, September 11. Global InsurTech investments sharply increased in Q2 2017 as innovation becomes the new normal for reinsurers. Retrieved January 19, 2018, from https://www.pwc.co.uk/press-room/press-releases/Global-InsurTech-investments-sharply-increased-in-Q2-2017-as-innovation-becomes-the-new-normal-for-reinsurers.html

Qin, Y., Sheng, Q. Z., Falkner, N. J. G., Dustdar, S., Wang, H., & Vasilakos, A. V. 2016. When things matter: A survey on data-centric internet of things. Journal of Network and Computer Applications, 64, 137–153. https://doi.org/10.1016/j.jnca.2015.12.016

Radesky, J. S., Schumacher, J., & Zuckerman, B. 2015. Mobile and Interactive Media Use by Young Children: The Good, the Bad, and the Unknown. Pediatrics, 135(1), 1–3. https://doi.org/10.1542/peds.2014-2251

Reed, C., Kennedy, E., & Silva, S. 2016. Responsibility, Autonomy and Accountability: Legal Liability for Machine Learning (SSRN Scholarly Paper No. ID 2853462). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2853462

Rid, T., & Buchanan, B. 2015. Attributing cyber attacks. Journal of Strategic Studies, 38(1–2), 4–37.

Ritchey, T. 2011. General Morphological Analysis (GMA). In T. Ritchey (Ed.), Wicked Problems – Social Messes. Decision Support Modelling with Morphological Analysis (Vol. 17, pp. 7–18). Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-642-19653-9_2

Rolls-Royce. 2016. Autonomous ships. The next step (pp. 1–8). Westhampnett: Rolls-Royce. Retrieved from http://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/rr-ship-intel-aawa-8pg.pdf

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. 2017. Content Analysis of Cyber Insurance Policies (No. WR-1208). San Francisco: RAND Corporation. Retrieved from https://www.rand.org/pubs/working_papers/WR1208.html

Sampson, H., Ellis, N., Acejo, I., & Turgo, N. 2017. Changes in seafarers' health 2011-16: A summary report (p. 22). Cardiff: Seafarers International Research Centre. Retrieved from http://www.sirc.cf.ac.uk/Uploads/Publications/Changes%20to%20seafarers'%20health%202011-2016.pdf

Scardovi, C. 2017. Transformation in Insurance. In Digital Transformation in Financial Services (pp. 163–185). Cham: Springer. https://doi.org/10.1007/978-3-319-66945-8_10

Schwab, K. 2016, January 14. The Fourth Industrial Revolution: what it means and how to respond. Retrieved July 17, 2018, from https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Select Committee on Artificial Intelligence. 2018. AI in the UK: ready, willing and able? (pp. 1–183). London: House of Lords. Retrieved from https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf

Senate of the United Staates. 2017. Internet of Things (IoT) Cybersecurity Improvement Act 2017 (pp. 1–20). Washington D.C.: Senate of the United States. Retrieved from https://www.congress.gov/115/bills/s1691/BILLS-115s1691is.pdf

Serafin, C. 2018. A Policyholder's Guide to IoT Claims Coverage. Risk Management, (January/February), 8–9.

Shaikh, F. K., Zeadally, S., & Exposito, E. 2017. Enabling Technologies for Green Internet of Things. IEEE Systems Journal, 11(2), 983–994. https://doi.org/10.1109/JSYST.2015.2415194

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. 2016. Taxonomy of information security risk assessment (ISRA). Computers & Security, 57, 14–30. https://doi.org/10.1016/j.cose.2015.11.001

Spring, T. 2016, December 8. Some Solar Power Meters are Vulnerable to Command Injection Attacks. Retrieved June 19, 2018, from https://threatpost.com/solar-power-firm-patches-meters-vulnerable-to-command-injection-attacks/122324/

SRI Consulting Business Intelligence. 2008. Six Technologies With Potential Impacts on US Interests Out to 2025 (No. CR 2008-07) (p. 48). Washington D.C.: National Intelligence Council. Retrieved from https://fas.org/irp/nic/disruptive.pdf

Tanczer, L., Blythe, J., Yahya, F., Brass, I., Elsden, M., Blackstock, J., & Carr, M. 2018. Summary literature review of industry recommendations and international developments on IoT security (pp. 1–18). London: Department for Digital, Culture, Media & Sport; PETRAS IoT Hub. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/686090/PETRAS_Literature_Review_of_Industry_Recommendations_and_International_Developments_on_IoT_Security.pdf

Tanczer, L., Brass, I., Elsden, M., Carr, M., & Blackstock, J. (forthcoming). The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. In R. Ellis & V. Mohan (Eds.), Rewired: Cybersecurity Governance. Wiley.

Tanczer, L., Carr, M., Brass, I., Steenmans, I., & Blackstock, J. 2017. IoT and Its Implications for Informed Consent (pp. 1–36). London: PETRAS IoT Hub; STEaPP. Retrieved from http://ssrn.com/abstract=3117293

Tanczer, L., Patel, T., Parkin, S., & Danezis, G. 2018. Response by the "Gender and IoT" Research Team: The Implications of the Internet of Things (IoT) on Victims of Gender-Based Domestic Violence and Abuse (G-IoT) (pp. 1–12). London: University College London. Retrieved from https://www.ucl.ac.uk/steapp/research/projects/digital-policy-lab/domestic-violence-consultation

Tanczer, L., Steenmans, I., Elsden, M., Blackstock, J., & Carr, M. 2018. Emerging risks in the IoT ecosystem: Who's afraid of the big bad smart fridge? In Living in the Internet of Things: Cybersecurity of the IoT - 2018. London, UK: IET. https://doi.org/10.1049/cp.2018.0033

Tanczer, L., Yahya, F., Elsden, M., Blackstock, J., & Carr, M. 2017. Review of International Developments on the Security of the Internet of Things (pp. 1–37). London: PETRAS IoT Hub; STEaPP.

Tzounis, A., Katsoulas, N., Bartzanas, T., & Kittas, C. 2017. Internet of Things in agriculture, recent advances and future challenges. Biosystems Engineering, 164, 31–48. https://doi.org/10.1016/j.biosystemseng.2017.09.007

UK Government Chief Scientific Adviser. 2014. The Internet of Things (Blackett Review): Making the Most of the Second Digital Revolution. London: Government Office for Science. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf

UL. 2017. Cybersecurity Considerations for Connected Smart Home Systems and Devices (pp. 1–10). Northbrook, Illinois, United States: UL. Retrieved from https://www.ul.com/consumer-technology/en/knowledge-center/cybersecurity-considerations-for-connected-smart-home-systems-and-devices/

UNEP. 2015. Options for decoupling economic growth from water use and water pollution (Report of the International Resource Panel Working Group on Sustainable Water Management) (pp. 1–78). Nairobi, Kenya: United Nations Environment Programme. Retrieved from https://www.researchgate.net/publication/301807298_UNEP_2015Options_for_decoupling_economic_growth_from_water_use_and_water_pollution_Report_of_the_International_Resource_Panel_Working_Group_on_Sustainable_Water_Management

van Rij, V. 2010. Joint horizon scanning: identifying common strategic choices and questions for knowledge. Science and Public Policy, 37(1), 7–18. https://doi.org/10.3152/030234210X484801

Vodafone, Analysys Mason, & Circle Research. 2017. The IoT Barometer 2017/18 (pp. 1–36). Newbury: Vodafone. Retrieved from https://www.vodafone.com/business/news-and-insights/white-paper/iotbarometer

Wickens, C. D., & Dixon, S. R. 2007. The benefits of imperfect diagnostic automation: a synthesis of the literature. Theoretical Issues in Ergonomics Science, 8(3), 201–212. https://doi.org/10.1080/14639220500370105

Williams-Grut, O. 2017, September 1. Investment in one area of fintech is up more than 2500% year-on-year. Retrieved January 19, 2018, from http://uk.businessinsider.com/accenture-insurtech-investment-2017-9

Wolff, J. 2018, June 4. Cyberinsurance Tries to Tackle the Unpredictable World of Hacks. Retrieved April 15, 2018, from https://www.wired.com/story/cyberinsurance-tackles-the-wildly-unpredictable-world-of-hacks/

Yang, H., Lee, W., & Lee, H. 2018. IoT Smart Home Adoption: The Importance of Proper Level Automation. Journal of Sensors, 2018, 1–11. https://doi.org/10.1155/2018/6464036

Yang, J., Wang, C., Zhao, Q., Jiang, B., Lv, Z., & Sangaiah, A. K. 2018. Marine surveying and mapping system based on Cloud Computing and Internet of Things. Future Generation Computer Systems, 85, 39–50. https://doi.org/10.1016/j.future.2018.02.032

Yang, L., Yang, S.-H., Magiera, E., Froelich, W., Jach, T., & Laspidou, C. 2017. Domestic water consumption monitoring and behaviour intervention by employing the internet of things technologies. Procedia Computer Science, 111, 367–375. https://doi.org/10.1016/j.procs.2017.06.036

Yang, Y., Lee, T., Lee, Y., Choi, J., Park, E., & Lim, H. 2017. Implementation of infants risk detection sensing system using IoT. AIP Conference Proceedings, 1836(1), 020073. https://doi.org/10.1063/1.4982013

Zhang, Y., & Wen, J. 2017. The IoT electric business model: Using blockchain technology for the internet of things. Peer-to-Peer Networking and Applications, 10(4), 983–994. https://doi.org/10.1007/s12083-016-0456-1

Icons

Icons in this report are from The Noun Project, and include: home wifi, Ben Davis; Falling Cards, Andrew Hainen; Scale, purplestudio; insurance, Maxim Basinski; Data, Guilhem; approval, Thomas' designs; argue, Gianni - Dolce Merda; wifi, Priyanka; Stamp, IYIKON; Certificate, Creative Stall; Brain, Symbolon.