Editors of the Cybersecurity of the Internet of Things: PETRAS Stream Report

Dr Kruakae Pothong, Dr Irina Brass and Dr Madeline Carr

Authors by chapter:

01 Standards, Governance and Policy
   Irina Brass, Kruakae Pothong, Leonie Tanczer, Madeline Carr

02 Safety and Security
   Razvan Nicolescu, Barnaby Craggs, Emil Lupu, Awais Rashid

03 Privacy and Trust
   Carsten Maple, Susan Wakenshaw, Mariarosaria Taddeo

04 Harnessing Economic Value
   Petar Radanliev, Razvan Nicolescu, David De Roure, Michael Huth

05 Adoption and Acceptability
   Joseph Lindley, Sara Cannizzaro, Rob Procter, Paul Coulton

With design by Creative Range and Michael Stead

The report should be referenced as follows:


If you would like to reference a specific chapter in the report, please use the following format:


© PETRAS Internet of Things Research Hub 2019. All rights reserved.
HUB PARTNERS

SPOKE PARTNERS

EXTERNAL PARTNERS

CONSTELLATION OF PROJECTS

CHALLENGE STREAMS

Standards, Governance and Policy

Harnessing Economic Value

Safety and Security

Privacy and Trust

Adoption and Acceptability

Transport and Mobility

Supply and Control Systems

Healthcare

Ambient Environments

Infrastructure

EPSRC

IoT

THALES

micro-bit

TTI

osmotic

HMGCC

TOSHIBA

BBC

HARCA

Zoological Society

TRL

CATAPULT

British Gas

NCA

INTERDigital

ZTE

Home Office

University of Bristol

Lancaster University

Imperial College London

Cardiff University

Amidus

NEC

CONCENTRA

GRAND LONDON AUTHORITY

Raytheon

NSPCC

Which?

SIEMENS

nasa

TPD

Office of the National CIO

Office of the National CDO

OFFICE OF THE NATIONAL CIO

Office of the National CDO

OFFICE OF THE NATIONAL CIO

Office of the National CDO

OFFICE OF THE NATIONAL CIO
It is my pleasure to present this final report for the five ‘Streams’ of the three year PETRAS Research Hub for the Cybersecurity of the Internet of Things. In a unique configuration, PETRAS has brought together social and physical scientists to work collaboratively on addressing some of the challenges and questions around the cybersecurity of the Internet of Things. Questions like – What perception has society of IoT cybersecurity risks? How is behaviour affected by IoT technology? How is technology influenced by human factors? What can developers, government and society do to increase value and mitigate risk from IoT technologies?

In addition to assembling a substantial corpus of socio-technical evidence captured through more than 50 research projects and demonstrators over 100 person-years of effort, PETRAS has addressed knowledge needs under five, policy-related headings which we have referred to throughout the project as ‘Streams’. These are: Privacy and Trust, Adoption and Acceptability, Safety and Security, Standards, Governance and Policy, and Harnessing Economic Value.

Dedicated socio-technical research teams have worked on each Stream to meet a number of objectives. They carried out research specific to those particular aspects of the PETRAS research agenda. In addition, these teams offered focused
support to individual research projects where they intersected with the Streams. Finally, the Streams also drew out findings from the projects to help build a rich profile of conclusions informed by diverse studies, approaches and topic areas. This report offers a synthesis of all of this work, bringing together research findings from across PETRAS.

In introducing this report, I am delighted to say that independent assessors consider that PETRAS has greatly exceeded expectations in terms of the quality and coverage of its outputs, engagement with private and public sectors, and impact. PETRAS research leads and associates have created a robust platform of cross-disciplinary understanding and capability, which promises to nurture further work establishing the UK's national capability and pre-eminence in Internet of Things cybersecurity. A 'User and Research Partner' community of more than 120 organisations has been created, and a recent independent study has shown that over 1,000 external organisations are aware of PETRAS outputs, with many drawing upon them.

PETRAS has been methodologically and organisationally innovative. It is an exemplar of integrated work across social and physical science domains, demonstrating important possibilities and benefits. Some of these are most evident where product design ‘futurists’ have worked with behavioural and technology experts in fields such as telecare, medical devices and consumer IoT products.

Further indications of value and impact are evident in the appetite that UK government departments and agencies have shown for working with PETRAS. For example, the Department for Digital, Culture, Media and Sport used PETRAS behavioural science insights in writing its Secure by Design paper, and the National Cyber Security Centre (NCSC) has commissioned studies into emerging technologies and applications of IoT in industrial automation. The National Physical Laboratory is also watching PETRAS outcomes with a view to enhancing the security and provenance attribution of digital measurements. It has become clear over the past three years of PETRAS research that both regulation and procurement have roles to play in guiding standards and their adoption. Government has an important role in shaping, accrediting and procuring against standards so that security is not a post-hoc ‘fix’.

It is evident that PETRAS has moved the IoT cybersecurity debate forward. The security of IoT systems is now widely discussed, and responsibility for this in the UK is now taken up by DCMS. The role of cellular networks as IoT infrastructure, particularly 5G, is also much better appreciated. IoT standards in the UK are at an early stage of development and are being formulated ahead of proven best practice. PETRAS Stream researchers have provided a strong input to the establishment of standards for the IoT, leading the British Standards Institution’s activity in this area.

I hope this report from the PETRAS streams will catalyse further debate to inform policy options that can be developed by government and industry, making the use of the IoT safe and trustworthy, and maximising its economic value to the UK.
CONTENTS

INTRODUCTION .........................................................................................................................02

01 STANDARDS, GOVERNANCE AND POLICY ........................................................................05
   Irina Brass, Kruakae Pothong, Leonie Tanczer, Madeline Carr

02 SAFETY AND SECURITY ..................................................................................................25
   Razvan Nicolescu, Barnaby Craggs, Emil Lupu, Awais Rashid

03 PRIVACY AND TRUST .....................................................................................................47
   Carsten Maple, Susan Wakenshaw, Mariarosaria Taddeo

04 HARNESING ECONOMIC VALUE ....................................................................................75
   Petar Radanliev, Razvan Nicolescu, David De Roure, Michael Huth

05 ADOPTION AND ACCEPTABILITY ....................................................................................93
   Joseph Lindley, Sara Cannizzaro, Rob Procter, Paul Coulton

CONCLUSION: THE FUTURE OF IOT ......................................................................................109

APPENDIX 01: PETRAS PROJECTS AND STREAM ALIGNMENT .............................................113

APPENDIX 02: LIST OF PETRAS PROJECTS REFERENCED IN THIS REPORT .........................117
INTRODUCTION

The PETRAS Cybersecurity of the Internet of Things Research Hub is a consortium of leading UK universities that have been working together over the past three years to explore critical issues in the privacy, ethics, trust, reliability, acceptability, and security of the Internet of Things. Funding for the Hub included a £9.8 million grant from the Engineering and Physical Sciences Research Council (EPSRC), which was boosted by partner contributions of over £14 million across the lifespan of the Hub. This project was also run in collaboration with IoTUK.
The PETRAS Cybersecurity of the IoT Hub is led by UCL and includes 10 other UK universities: Imperial College London, Lancaster University, University of Oxford, University of Warwick, Cardiff University, University of Edinburgh, University of Southampton, University of Surrey, University of Bristol and Newcastle University.

The research agenda of PETRAS was first set out in a report by the UK Chief Scientific Adviser. The Internet of Things: Making the most of the Second Digital Revolution report (Blackett Review, 2014) highlighted both the opportunities and challenges of the Internet of Things (IoT), urging the government to take the lead in fostering and promoting the adoption of IoT. It highlighted eight areas for action: commissioning of IoT products and services, spectrum and network infrastructure to support IoT deployment, skills and research, data, regulation and legislation, trust and coordination.

Following the review, the PETRAS Research Hub was established to investigate critical issues concerning Privacy, Ethics, Trust, Reliability, Acceptability and Security (PETRAS) pertaining to the Internet of Things.

The PETRAS Hub features a uniquely interdisciplinary approach to investigating the benefits and challenges arising from the deployment and adoption of the IoT across many sectors and domains. PETRAS brought together international research leaders, cross-sectoral industrial users, government agencies and NGOs. Research carried out within the hub was organised around five ‘Streams’: Standards, Governance and Policy, Safety and Security, Privacy and Trust, Harnessing Economic Value, and Adoption and Acceptability. These Streams transect diverse sectors and application areas, including consumer goods, healthcare, ambient environments, infrastructure, supply and control systems, and transport and mobility. The investigation of each Stream was directed by two research leaders, providing both technical and social expertise, and supported by post-doctoral researchers.

Findings from PETRAS research highlight opportunities for both the economy and society, including emerging business trends. However, key overarching challenges remain:

- **Capturing the socio-economic benefit of the IoT to the UK and global economy**: At the moment, we have competing projections about the IoT adoption rate across various sectors, the likely direct economic contribution to the UK economy and its indirect effects in terms of value added to several sectors. Equally, we need clearer measures to understand and assess the direct and indirect effects that a suboptimal level of IoT cybersecurity might have for the UK and global economy.

- **The complexity of IoT systems**: The interconnected nature of IoT implementations and the blurring lines between safety and security mean that risk assessment and evaluation in the IoT is extremely challenging. New models for dynamic risk assessment will be called for if the IoT is to develop with sufficient levels of security.

- **The IoT is a dynamic innovation undergoing constant and rapid advancement**: Responses to this advancement and the consequent emerging issues requires more agile and innovative governance approaches that are still evolving. These challenges require careful consideration of the design of IoT products, services and systems as well as the design of policies and adaptive mechanisms to govern the IoT at the domestic and international level. Details of these key findings will unfold through the Stream report in the following chapters.
Insurance policies can provide incentives for implementing minimum security standards and safeguards against a range of IoT-specific threats despite challenges in identifying the suitable methods for basic cyber risk assessment and liability models in complex digital ecosystems.

A systems perspective to the development of IoT standards is required in order to tackle security risks across the main IoT components: endpoints, networks and cloud services. However, the IoT standards landscape remains fragmented and unaligned.

More effective interaction between the international policy and technical communities is urgently needed if transnational IoT risks and vulnerabilities are to be effectively mitigated and cross-border trade facilitated.

Data trust models that incentivise transparency and accountability in data exchanges between data subjects, controllers and processors, as well as clear data sharing policies, are in high demand.

A public consultation on corporate responsibilities is required to prevent negative consequences from data processing, profiling or choices and avenues to opt out of any data collection.
STANDARDS, GOVERNANCE AND POLICY
SAFETY AND SECURITY
PRIVACY AND TRUST
HARNESSING ECONOMIC VALUE
ADOPTION AND ACCEPTABILITY

Data Sharing in the IoT (PEDASI) Demonstrator
IoT Multi-disciplinary Standards Platform (IoT-MSP)
Developing a Consumer Security Index for Consumer IoT Devices (CSI)
House Training the Internet of Things (HTIoT)
Cyber Risk Assessment for Coupled Systems (CRAC)
National and International Policy for Critical Infrastructure Cybersecurity (NICP)
Designing Dynamic Insurance Policies using IoT (DDIP-IoT)
The Internet of Every Things (P2P-IoET)
Gender & IoT (G-IoT)
INTRODUCTION

The IoT ecosystem is characterised by ‘a proliferation of visible and hidden sensors that collect and transmit data, systems that process, interpret and make use of the aggregate information, and actuators that, on the basis of this information, take action without direct human intervention’ (Tanczer et al., 2019). The added ability of connected objects to sense and communicate with other objects and people presents exciting opportunities for society and the economy.

However, the IoT also has the potential to introduce new technical, social, economic and policy challenges. These include, for instance, concerns about the scope and misalignment between current security, privacy, safety and liability laws. The connectivity aspect of the IoT means that these problems are not contained in any specific area or jurisdiction and, consequently, are not easily dealt with by a single government. Instead, they weave across products, industry verticals and sectors (e.g. medical, automotive, critical infrastructure, etc.) and, invariably, across borders. A holistic view across the diverse IoT ecosystems reveals shortcomings as well as tensions in existing modes of governing disruptive digital technologies and managing their intended and unintended consequences.

Given these challenges and the complexity of the IoT, changes to existing principles and practices are required, particularly the ‘culture of security’ around emerging digital technologies. In addition, skills development and training become paramount. Responding to these requirements, the Standards, Governance and Policy (SGP) Stream of the PETRAS IoT hub investigated whether current governance approaches are adequate to promote the benefits that the IoT promises, while mitigating the complex and interdependent challenges that it raises. The SGP work focuses on three core elements, henceforth referred to as the Research Focus (RF):

a) Changes to liability, responsibility and the implementation of individual consent, with a particular focus on the respective roles of IoT manufacturers, service providers, the insurance sector and governments in the governance of the IoT;

b) Changes to the cultures of security that will be required in the IoT ecosystem; and

c) The adequacy and effectiveness of complementary modes of governing IoT such as standards, certification schemes, non-binding best practices, international norms, and mandatory rules and regulations.

In examining these elements, the SGP Stream worked closely with the Department for Digital, Culture, Media and Sport (DCMS) to support the development of the Code of Practice for Consumer IoT Security, providing a review of existing standards, best practices and international avenues suitable for managing IoT security in a globally coordinated manner. We also worked closely with the IoT-1 Committee of the British Standards Institution (BSI) to inform the development of standards for IoT security, privacy and interoperability, and to understand the needs and concerns of SMEs operating in the IoT space (see RF3, Issue 1).

In addition, our team collaborated with the Warwick Manufacturing Group and the international law firm Pinsent Masons to understand the challenges of regulating complex cyber-physical systems such as connected and autonomous vehicles (CAVs), and to explore the difficulties of implementing the principle of freely given, informed and unambiguous consent in these complex environments. This collaborative engagement culminated in a report on the IoT and its implications for informed consent, as well as further research into the practical reality of data protection laws (see RF1 Issue 3). To investigate issues of responsibility, risk and liability, we partnered with
Lloyd's of London to draw on expertise within the insurance sector. Through intensive engagement with their underwriters and by utilising unique investigation methods in futures and foresight, we generated a report that provides insight into the future of the IoT and the role that insurance policies can play as an instrument for managing challenges and opportunities in the IoT (see RF1 Issue 1).

Finally, we collaborated with international partners such as the World Economic Forum (WEF), the European Union Agency for Network and Information Security (ENISA), the Asia-Pacific Network Information Centre (APNIC) and the Forum of Incident Response and Security Teams (FIRST) to explore how global practices and approaches to the cybersecurity of the IoT are developing and can be transformed. This focus on the diverse ‘cultures of security’ adopted across different international and transnational organisations was highlighted in several presentations and workshops, including at the UN Internet Governance Forum (UN IGF) and the Institution of Engineering and Technology (IET)/PETRAS ‘Living in the IoT’ Conference, which fostered engagement between the global policy community and technical cybersecurity experts (see RF3 Issue 2).

**Insights**

The research conducted by the SGP Stream has highlighted that policy-makers, the international community and industry players are more aware of, and indeed, taking action to respond to, some of the main cybersecurity, data protection and safety challenges raised by the IoT. In the UK, some of these steps include the development of non-binding Codes of Practice and Guidelines by Department for Digital, Culture, Media and Sport (DCMS) on IoT consumer goods and by the Department for Transport (DFT) on connected and autonomous vehicles in the UK; the EU Cybersecurity Act, as well as the adoption of the GDPR and the NIS Directive; the growing number of market-driven IoT guidelines and standards, as reported by DCMS, ENISA and The US National Institute of Standards and Technology (NIST); and the proposal by the WEF for agile governance of emerging digital technologies as key drivers of the Fourth Industrial Revolution.

While these initiatives are valuable in highlighting the main risks associated with the IoT and in proposing baseline principles and guidelines for responsible cybersecurity and trustworthy IoT, they also reveal a number of blind spots and limitations in the current governance of IoT risks:

1) Most of the proposed IoT cybersecurity guidelines and best practices remain non-binding, requiring market take-up. This implies considerable adoption and monitoring costs especially for small and medium enterprises innovating in this space (Brass et al 2019., forthcoming);

2) The increased adoption of the IoT in private environments, such as the home, raises new concerns about the protection of personal information and the right to privacy, as well as the potential misuse of this technology against vulnerable individuals and groups (Tanczer et al., 2018);

3) There is a growing need for technical experts and the policy community to work together at the domestic and international level in order to better communicate what informs their decision-making about IoT security and to better understand the inherent trade-offs of their practices and actions (Carr et al., 2018).

Overall, the SGP Stream found that there is a clear need to consider and design new governance mechanisms that acknowledge the expertise, capacity and contribution of key stakeholders in the IoT ecosystem, in order to ensure a proportionate and flexible way of responding to new trends in IoT market development.

Some of these trends have been captured by work that has been carried out in several projects across the PETRAS Research Hub, especially a trend towards a marketplace for data and emerging IoT business models and alliances. These offer
opportunities as much as risks, creating new demands and challenges for a wide range of stakeholders. Thus, the evolving IoT ecosystem requires policies, governance models and stakeholders to adapt – not only to open up economic and efficiency benefits, but most importantly to protect society from harmful technological changes, inherent biases and potential technological abuse.

A Marketplace for Data

In the sophisticated and interconnected IoT ecosystem, data sets are gaining in value and consequently there is growing interest in data exchanges and commercialisation. Connected to data markets are interests in the free flow of data, abilities to negotiate data flows and openness. Our research and findings highlight that transparency, accountability and trust will be key to fostering such business models in a responsible and ethical manner and to cater to users’ associated interests – drawing here on a number of PETRAS projects, including the Data Sharing in the IoT (PEDASI) Demonstrator, the IoT Multi-disciplinary Standards Platform (IoT-MSP), Developing a Consumer Security Index for Consumer IoT Devices (CSI), House Training the Internet of Things (HTIoT), Cyber Risk Assessment for Coupled Systems (CRAC) and National and International Policy for Critical Infrastructure Cybersecurity (NIPC).

At the moment, there is demand for data trust models that incentivise transparency and accountability in the exchange of data between data providers and data consumers, as well as clear data sharing policies. In relation to these values and interests, the SGP Stream, in collaboration with the mentioned PETRAS projects, identifies six priority challenges:

1) absence of assessment models to account for both cybersecurity risks and the economic impact of information security breaches,
2) the advancement of tech-facilitated crimes,
3) the lack of data trust models,
4) limited individual awareness about data collection, data sharing practices between data controllers, processors and third parties and their negotiation power,
5) the lack of clarity in data ownership,
6) the gap between policy and its technical implementation.

Limited awareness about data collection and sharing, combined with uncertainties around data trust models and data ownership, undermine the capability of individuals – who are both data providers and consumers – to negotiate their terms of data sharing, to develop trust in it and to perceive incentives for doing so. As data appreciates in value, cyber risk assessments that do not factor in the measures to prevent as well as covering the costs of arising data breaches are rendered irrelevant and unreliable. The gap between data protection policies and their technical implications could result in adverse effects for consumers and inefficiencies in investment, as well as a need for additional resources to support the data marketplace. Tech-facilitated crimes highlight the need for more criminology research and funding to keep pace with technology changes. Failure to do so would undermine citizen and consumer welfare.

To address these issues, we argue that all stakeholders form part of the solution. Concerning awareness and skills, our research and other findings from PETRAS projects suggest that a change in the national curriculum relating to computer science, policy and law is required. We see the government playing a key role in this endeavour. However, industries, charities and consumer associations also have to play a part in providing informal education, support and guidance for individual users, frontline responders and victims/survivors of tech-facilitated crimes and abuses (Tanczer et al., 2018b). The CSI project investigated different labelling schemes for IoT devices (Blythe and Johnson, 2018), offering a clear mechanism to reduce the burden currently placed on consumers. The scheme also serves as further incentive for manufacturers to comply with baseline IoT security requirements. Government is seen as best placed to
implement the labelling scheme to ensure effective enforcement in the market, conformity assessment, as well as aligning the scheme with the broader role of cybersecurity certification, currently explored in the EU Cybersecurity Act. Findings from this project further highlight the need for increased transparency and accountability about software updates through the entire lifecycle of an IoT device. To realistically account for the value of data in risk assessments, an integrated cyber risk impact assessment approach, accounting for both the economic and the cyber-physical impacts of risks in the IoT (Radanliev et al., 2018b), is required. Government and standards development organisations should make this integrated cyber risk assessment approach a prerequisite as they plan for the standardisation of IoT (Radanliev et al., 2019a).

For the issues relating to trust and power dynamics in the relationships between businesses and individuals, we anticipate that new forms of corporate social responsibility will evolve as governance models that are sufficiently agile to cater to the requirements of various industry sectors in which IoT systems are incorporated. This would require corporations to work in close partnership with government and across borders. As for the impact of IoT on citizen welfare, the House Training the Internet of Things (HTIoT) project suggests that an IoT Discrimination Act and public consultation on corporate responsibilities are required to prevent the negative consequences from data processing, profiling or choices and avenues to opt out of any data collection. These efforts require government action and public engagement to ensure responsible industrial practices.

New Business Models and Convergence of Market Sectors

Connected to the trends towards a marketplace of data are emerging business models and increased technological and market convergence. An example of such development is the Mobility Open Blockchain Initiative (MOBI). This is an alliance of car manufacturers, technology corporations, financial technology (FinTech) companies, non-profit organisations and governments with interests in standards development and acceleration of IoT, blockchain adoption, distributed ledger and other related technologies in the automotive sector. This alignment works towards a broader convergence between market sectors such as car manufacturing, software, hardware, financial (e.g. insurance) and emerging digital technologies. One common aim is to create added value by improving the environmental impact of each of these technologies and the overall quality of life. For instance, smart cars can perform bank brokerage for drivers or other parties while driving. The dynamics and value of such convergence requires further investigation to enable a broader range of stakeholders and industries to capitalise on opportunities (e.g. data trade, energy consumption, new integrated and dynamic financial services) and to be aware of the important social consequences of these changes.

These new dynamics at both market and technology levels blur the traditional boundaries between providers and consumers of services, challenging existing business models. These dynamics and values also further complicate existing notions of trust and trustworthiness in the complex IoT ecosystem, requiring stakeholders to rethink and clarify these concepts (Brass et al., 2018a).

Findings from the PETRAS project Designing Dynamic Insurance Policies using IoT (DDIP-IoT) highlight the risks of market consolidation as well as opportunities for new entrants with expertise in big data and the insurance sector. Vertical convergence in provision of product and services was observed, for example, in Volvo, a major car manufacturer venturing into an insurance market for connected and autonomous vehicles. This type of convergence can introduce new pressure on dominant insurers (e.g. by changing their data sharing practices, bringing in critical expertise in artificial intelligence). Such convergence requires regulations to adapt to the changing landscape. This conclusion is also
supported by evidence from the NIPC project, linking the interests in data trade with evolving business models, manifested in ports and supply chains which often operate across borders. This highlights the need for international cooperation on cybersecurity and for the construction of digital rights frameworks.

Furthermore, successfully tackling these issues requires new standards, further regulatory alignment (Brass qtd in Royal Society, 2017a) and international cooperation. Our SGP research shows that standards can play an important role in providing degrees of certainty for both businesses and users, by informing the notions of IoT trustworthiness and reinforcing consumer trust. Regulations also need to adapt in order to bridge the misalignment between security, safety, product liability and data protection principles and practices, and to provide clarity for all entities in the IoT ecosystem, from consumers to manufacturers.

**A systems perspective to the development of IoT standards is required in order to tackle cybersecurity risk across the main IoT components: endpoints, networks and cloud services. New risks assessment standards are needed to ensure responsible cybersecurity practices across the IoT supply chain. However, the IoT standards landscape remains fragmented and unaligned.**

To facilitate cross-border trade in goods, services and data, findings from the NIPC project (Carr et al., 2018) suggest that fostering more effective engagement between the international cybersecurity policy community and their technical counterparts in the technical sector is urgently needed if transnational risks and vulnerabilities are to be effectively mitigated. On the technical front, the CRACS project finds that tackling cybersecurity risks requires standardisation of digital components in IoT supply chains to prevent these components from being compromised. Such standardisation serves to clarify the design of individual IoT digital components. This in turn supports the development of capability for autonomous cognitive decisions in defence against cyberattacks (Radanliev et al., 2019-b).

SGP research also finds that more effective cooperation between the cybersecurity policy community and their technical counterparts is needed (Tanczer et al., 2018a). The demands for standards, regulations, international cooperation, combined with the absence of consensus on leadership on these issues, present opportunities for the UK to take a leadership role in shaping the debates and facilitating international agreements to ensure a safe and secure IoT. The UN IGF, the International Telecommunication Union (ITU), the Organisation for Economic Co-operation and Development (OECD), as well as the WEF, are already facilitating platforms to generate broader initiatives on IoT best practices and standards. There is scope for the UK to set the IoT security agenda in these forums to achieve wider political consensus within the G7 and G20 with a view to moving towards greater cooperation. However, this can only be effective if it is pursued in collaboration with other stakeholders, especially the technical community.

**RF1: RISK, LIABILITY AND CONSENT**

The SGP Stream’s research on risk, liability and consent identified diverse layers of responsibility and relevant actors to the security and safety of the IoT. Aligned with international developments and research in this space, the SGP Stream studied the ways in which the IoT challenges existing legislative frameworks and risk management practices, and stretches our understanding of how to implement freely given, informed and unambiguous consent in an inherently interdependent environment. Throughout our research we actively worked with core stakeholders who design, deploy and regulate IoT systems. We sought to detect where responsibilities and critical uncertainties remain and identified the insurance sector as a potential influential stakeholder with the capacity to set security thresholds due to its expertise in the assessment of risk.
Issue 1: Liability and Insurance

PETRAS SGP Stream research demonstrated how new cyber-physical vulnerabilities require new conceptualisations and classifications of risks. The IoT creates multi-dimensional vulnerabilities and threats that stretch from devices to communication networks to platforms, services and data (Tanczer et al., 2018c). They challenge existing risk management frameworks (Nurse et al., 2017) and introduce new demands on existing legislation and regulations (Brass et al., 2017).

As a result of this research, the SGP Stream provided evidence to a European Parliament hearing on the regulatory options available to close existing gaps in the product liability legislation (Tanczer et al., 2017a). The Stream stressed the need to reassess the responsibility of software vendors in the current environment that extensively relies on software operating on machines. At present, the EU liability regime is primarily focused on physical products and questions of damage and defectiveness. Software flaws and resulting failures and biases remain unaddressed. The research team suggested a comprehensive review of the framework and also proposed a hybrid approach to legislation, including a mix of voluntary measures and top-down regulation.

Parts of this proposal resonate with the recent creation of a common EU Cybersecurity Certification Framework (2018). The certification will be voluntary, but should make it easier for users to navigate between different technology offers, and for companies to carry out their business across borders.

Given the remaining uncertainties around liability, security and safety in complex cyber-physical systems (Brass et al., 2018b), the SGP Stream identified the potential of the insurance sector to address and mitigate emerging IoT risks. The insurance sector has a long-standing history of applying knowledge and science to balancing risk and costs in diverse sectors and settings (Young et al., 2016). Insurance policies can provide organisations with incentives to implement minimum security standards and can also provide cover against a range of IoT-specific threats. However, findings from the DDIP-IoT project highlight that the insurance industry is still struggling to make sense of the relevant issues, from methods for basic cyber risk assessment to liability models in complex ecosystems.

In the use of IoT-generated data to adjust access to insurance policies, transparency is needed to minimise the risk of exclusion or of limited choice.

Along similar lines, the SGP Stream’s collaboration with Lloyd’s of London reveals not only opportunities for the insurance industry but also risks, requirements and barriers that could affect the efficacy of insurance as an enforcement mechanism for liability, security and safety (see Box 1.1). This work exposed the need for transparency around using IoT-generated data to adjust access to insurance policies so as to minimise the risk of exclusion or of limited choice. In the DDIP-IoT project, the Imperial College team collaborated with the Lloyd’s Register Foundation, exploring how ‘real-time’ adjustable insurance policies can be designed and managed using IoT. These themes were also drawn out through the development of a new model for assessing economic impact of IoT cyber risk, executed by the team at Oxford University in the Impact Assessment Model for IoT (IAM) project. This work resulted in a series of recommendations for cyber risk assessment for IoT (Radanliev et al., 2018b) and for better understanding the economic impact assessment of IoT cyber risk (Radanliev et al., 2018a).
Issue 2: Consent

The capacity of IoT systems to collect, share, analyse, reuse (as well as act upon) generated data renders individuals’ management of their personal data more important than ever. The SGP Stream examined these issues through a workshop with IoT experts from the Warwick Manufacturing Group, Southampton University, Pinsent Masons and the Department for Transport. The workshop findings were captured in a report that analysed IoT’s implications for informed consent (Tanczer et al., 2017b). It concluded that the opaque data cycles of the IoT environment result in a lack of transparency and traceability of data flows, impinging on the data subjects’ ability to make informed decisions about their collected information. This fundamentally challenges conventional approaches to consent and data protection, which currently rely upon users having comprehensive knowledge of the handling of data and the consequences of the data collection.

These consent issues intersected with work carried out by the House Training the Internet of Things (HTIoT) project and the PEDASI Demonstrator. HTIoT demonstrates the competing interests in exercising control over personal data and in the capitalisation of such data through people’s scepticism about corporate probes in the guise of domestic IoT appliances. PEDASI addresses the lack of transparency and traceability affecting data subjects’ trust and incentives in sharing data, through a technical solution of data provenance and usage provenance craft, enabling data subjects to trace their data flows and their data use purposes.

The Internet of Every Things (P2P-IoET) project, through its assessment of existing regulatory and policy pathways around peer-to-peer energy trading, revealed that the lack of clarity on data protection is an obstacle to large-scale adoption of emerging digital technologies that are deployed alongside the IoT, such as blockchain. The extent to which data protection laws can address these issues remains to be seen. Complementary measures, such as voluntary standards, may be required to address the existing lack of legal clarity (Schneiders and Shipworth, 2018).

Additionally, the SGP Stream carried out an analysis of data protection laws accompanied by interviews with members of the Information Commissioner’s Office (ICO), Cabinet Office Privacy, Consumer Advisory Groups, the European Association for the Co-ordination of Consumer Representation in Standardisation (ANEC) and other consumer representatives. This revealed dilemmas in current data protection laws and a misrepresentation of the consumer’s knowledge and awareness of data flows, especially the right of individuals to exercise control over their personal data in complex cyber-physical systems. The prospective output of this ongoing research includes a publication (Pothong and Brass, in preparation), arguing for the creation of a new norm for communication between product manufacturers, software developers and service providers in the IoT industry. This should feature the connection between activities that generate data, data use and the implications of such use for what individuals value, in order to promote better awareness of data processing and incentivise people to exercise meaningful control over their data.
EMERGING IOT RISKS AND OPPORTUNITIES FOR THE INSURANCE SECTOR

In order to explore the emerging IoT risk and opportunity landscape for the insurance industry, the SGP Stream worked with Lloyd’s of London to develop future and foresight scenarios in four real-world contexts (maritime, smart home, critical water infrastructure and agriculture). The published output features in the Lloyd’s Emerging Risk Report series, outlining the benefits and operational requirements that the insurance sector will have to meet, in order to fully capitalise on IoT technologies and to prevent the exclusion and discrimination of potential policyholders. Barriers to the IoT’s full adoption include amongst others, the need for standardised data capture across different sectors and applications to ensure the necessary flexibility to accommodate granular and real-time data necessary for tackling information asymmetries and enhancing loss management.

MAIN PROJECT OUTPUTS


RF2: CULTURES OF SECURITY

The work on cultures of security explored the ‘multiple hands that touch the IoT’ and the awareness, culture and practices needed to tackle the challenges that IoT technologies pose – from a technical, economic and societal perspective. At the national level, the SGP Stream carried out an audit of cybersecurity skills training and awareness programmes developed by the UK Government, assessing the extent to which these initiatives responded to the new data protection and security challenges introduced by the IoT. At the international level, our research emphasised global governance approaches and mitigation strategies which are aimed at responding effectively to IoT-created challenges.

Issue 1: Training and Skills

The SGP Stream research on cybersecurity training and skills initiatives in the UK (Tanczer and Carr, 2017) echoed the efforts in the National and International Policy for Critical Infrastructure (NIPC) project to analyse the extent of current international cooperation on global cybersecurity policy for the IoT (Carr et al., 2018). In addition, the Cyberhygiene project studied the factors influencing consumers’ behaviour around actions that can mitigate risks from cyberattacks, particularly in the IoT environment (Blythe and Lefevre, 2018). Our work on the UK Government’s approach to cybersecurity skills development identified a lack of IoT-specific educational initiatives, which is increasingly important as these systems become more ubiquitous and widespread.

The SGP Stream also examined the level of awareness and dynamics relating to IoT’s potential to be misused and to disadvantage vulnerable groups. Specifically, the Gender and IoT (G-IoT) project at UCL as well as the IoT for Kids project at Lancaster University aimed to investigate the likely privacy and security challenges arising for victims of domestic abuse or children using IoT devices. For instance, the G-IoT project (see Box 1.2) outlined possible mitigating measures in a response to the UK Government’s ‘Transforming the Response to Domestic Abuse’ Consultation. Issues the G-IoT team raised included the need to expand the focus on technology-facilitated abuse in domestic and sexual violence cases to include emerging technologies such as the IoT. The research team also stressed the need to prepare both statutory and charitable support services for the challenges that these pervasive and ubiquitous technologies can pose for vulnerable communities. The CSI project conducted a systematic literature review of what crimes have and could be facilitated through consumer IoT devices in the future. A report from this review is in preparation.

This perspective resonates with the broader research agenda of the PETRAS IoT Hub, concerning the cultural changes resulting from the evolving IoT ecosystem, for which not only industry and government, but society at large, need to be prepared. The SGP Stream worked across the PETRAS hub and with key government stakeholders such as NCSC to address the difficult issue of consumer trust in IoT products and services. There was a common agreement across the hub that in order to ensure a sufficient level of consumer trust – which is required to optimise the advantages and benefits deriving from IoT systems – users need further information and skills, including sufficient understanding about the way the IoT functions.

Issue 2: Global Governance of IoT Security

For the international dimension, the SGP Stream coordinated a range of events and closely monitored the work of international organisations and representative stakeholders, including collaboration with the WEF, the European Union Agency for Network and Information Security (ENISA), Forum of Incident Response and Security Teams (FIRST) and the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG). The team worked very closely with DCMS and, together with colleagues from the Cyberhygiene and CSI project, contributed...
expert evidence and advice to the development of the UK Government’s 13 Secure by Design principles for consumer IoT products. A scoping literature review (Tanczer et al., 2018a) on the international developments on IoT by other global actors such as the UN, EU, Association of Southeast Asian Nations (ASEAN) and the Organisation for Economic Cooperation and Development (OECD) was published as Annex to the ministerial Secure by Design report (DCMS, 2018b).

This aspect of the SGP work is closely linked with the NIPC project. In collaboration with NIPC colleagues, the SGP Stream developed an IoT governance research repository for interested parties. This resource library is to be published online in 2019. It provides a database of IoT research taking place across the globe. The value of this database lies not only in the mapping of ongoing research in this space, but also in the identification of competing interests and tensions for policies and standards to govern the design of IoT products and services.

As part of this international outlook, the SGP Stream analysed technical and operational communities, especially Computer Security Incident Response Teams (CSIRTs) and their growing role in the security of the IoT and the internet’s infrastructure (Tanczer et al., 2018d). Through interviews with over 28 international CSIRT representatives, we highlighted the growing importance of this technical expert community in the active management of transnational cybersecurity risk. These and further insights were presented to and discussed with the international incident response community as well as policymakers and academics at the annual the United Nations Internet Governance Forum (UN IGF) in 2017.
VULNERABLE GROUPS AND THE IOT

Members of the SGP Stream together with colleagues from UCL Computer Science examined the gender-based implications of IoT in the context of domestic abuse and intimate controlling behaviour. The pilot study ran in collaboration with the London VAWG Consortium, the PETRAS IoT Hub and Privacy International and highlighted how emerging technologies such as ‘smart’ meters, locks and cameras expand risks for domestic violence victims. The research team proposed to expand the current focus on so-called ‘tech-abuse’ in both research and practice to account for IoT-facilitated forms of abuse and the work of bodies such as the NCSC. They also developed supporting material (a guide and resource list) for both statutory and charitable support services, and their work has been featured in outlets such as the E&T Magazine, the BBC or WIRED UK.

MAIN PROJECT OUTPUTS


RF3: STANDARDS, REGULATIONS AND MODES OF GOVERNANCE

Emerging technologies such as the IoT have both positive and negative disruptive effects on the businesses, organisations and sectors that develop, adopt or deploy them. The Blackett Review (HM Government, 2016) recognised the tensions between the intended consequences of emerging technologies such as new mobility services provided by connected and autonomous vehicles (CAVs), and their unintended consequences such as the risks they may pose to security, safety and overall roadworthiness. To mitigate these unintended consequences, the SGP Stream collaborated closely with key PETRAS partners and projects to map, analyse and assess the extent to which existing and emerging voluntary and mandatory regulations such as certification schemes and international norms are fit for purpose.

Issue 1: A Fragmented and Complex Standards Landscape

When faced with emerging technologies such as the IoT, governments usually consider whether the market is voluntarily creating or adopting best practices that set a responsible baseline of consumer and societal protection. This is mostly achieved through the development of de facto standards set by industry consortia and associations, or formal standards developed by national or international standardisation bodies. In order to assess the current state of play of these initiatives, the SGP Stream collaborated closely with the British Standards Institution (BSI) and DCMS to conduct a comprehensive review of the standards landscape for IoT security (Brass et al., 2018a).

The review identified three main trends in the current standards landscape for IoT security. First, the development of IoT security standards and guidelines has been led by industry consortia and associations, or formal standards developed by national or international standardisation bodies. In order to assess the current state of play of these initiatives, the SGP Stream collaborated closely with the British Standards Institution (BSI) and DCMS to conduct a comprehensive review of the standards landscape for IoT security (Brass et al., 2018a).

Group and informed the government’s decision to develop the Code of Practice for Consumer IoT Security (DCMS, 2018a).

Second, the review highlighted the difficulty of monitoring the adoption, implementation and effectiveness of IoT security standards and best practices by public and private organisations. The SGP Stream collaborated with the IoT Multidisciplinary Standard Platform project (PETRAS, BSI, IET) to conduct a survey designed to investigate the challenges organisations face in navigating the standards landscape relevant to the IoT. The findings of this review also led to the appointment of Dr Irina Brass as Chair of the BSI IoT/1 Committee and the publication of a BSI-PETRAS White Paper (Brass et al., 2019 forthcoming) that highlights key priority areas for SMEs that are trying to adopt IoT standards and best practices into their businesses, products and services.

Lastly, the review emphasised the difficulty of setting a baseline for IoT security across all the application domains and sectors. As an emerging technology, the IoT is blurring the boundaries between established standards and regulatory regimes for physical security, cybersecurity, safety, liability for defective products, data protection and trust/trustworthiness (Brass, qtd in Royal Society, 2017b). Several PETRAS projects have responded to this challenge that governments and standards development organisations are currently facing. The Consumer Security Index project (PETRAS, DCMS) has addressed the possibility of developing a labelling scheme for IoT security, by learning from existing labelling schemes in other sectors (e.g. food, energy) and by testing the impact of different labelling formats on consumer behaviours (Blythe and Johnson, 2018). The Ethics of Biomedical Big Data project proposed key ethical guidelines and best practices for IoT in high-risk sectors such as healthcare. Similarly, the IoT Observatory and the PETRAS PEDASI Demonstrator have highlighted the need for clearer and more transparent standards for data sharing and third-party use in order to ensure user trust.
The IoT-MSP Project investigated the obstacles to cybersecurity standards for IoT, and the potential development of a crowdsourced database and online portal to peer-review and assess the appropriateness, effectiveness and ease of implementing IoT relevant standards. In collaboration with the BSI, IET, the Digital Catapult and GCHQ, the IoT-MSP project conducted a survey of the main barriers to navigating, adopting and implementing standards. The results informed the SGP IoT Security Standards Landscape Review and led to a further PETRAS-BSI investigation into the main challenges that SMEs are facing when developing and designing secure IoT products and services (Brass, Pothong and Hasham, forthcoming, 2019).

The IoT-MSP project experimented with different configurations that would allow the creation of an open, transparent and customer-led platform for reviewing IoT standards. The project has already created a prototype of an interactive, user-friendly standards platform, which could be hosted by the BSI or the IET. The impetus for creating this platform is to provide standards review processes that allow customers to rate them on several criteria, such as ease of implementation, accessibility and effectiveness.

MAIN PROJECT OUTPUTS


Issue 2: The Need for International Coordination on IoT Security

With IoT becoming more widely adopted across multiple application areas and national borders there are pressing demands for international cooperation on cybersecurity. Domestic efforts can only be effective to a point and, in the IoT where complex global supply chains, integrated datasets and implications for physical as well as virtual safety and security feature, international approaches become more important than ever. In our analysis of the implications of the cybersecurity of the IoT for global governance, we looked closely at appropriate venues to facilitate international cooperation. In collaboration with the NIPC project, we produced an overview of international organisations and their focus on IoT cybersecurity, which supported and was published alongside the DCMS’s Secure by Design Code of Practice. Our investigation found that the IoT had not been factored into the global cybersecurity policy coordination taking place in most international forums. This is due in part to the failure to bring technical experts and policymakers together to address these issues, and in part to the difficulties inherent in addressing rapidly changing security problems through conventional governance mechanisms (Carr et al., 2018).

Issue 3: Adaptive Governance for IoT Trust and Trustworthiness

Emerging technologies such as the IoT raise important challenges for user trust. Businesses and governments are under pressure to demonstrate the trustworthiness of their organisational practices, products and services to users, consumers and society at large. Initiatives such as the Cyber Essentials Scheme were established to demonstrate cybersecurity trustworthiness by organisations operating in the UK. However, the IoT is an emerging technology, with cross-jurisdictional supply chains and data repositories that raise challenges to the siloed, slow-paced and misaligned domestic regulatory frameworks. The IoT requires collaborative adaptive governance that relies on the distributed capacity of several stakeholders.

From an industry perspective, the PETRAS B-IoT project has highlighted new market-driven models that are responding to the challenges around trustworthiness that coupled technologies such as the IoT, blockchain and automation raise for businesses. One example is an approach to significantly reduce high energy consumption for mining in blockchain applications by adapting existing technologies used in the automotive industry (Lundbaek et al., 2018). The regulatory and global regimes for governing emerging technologies also have to adapt (Brass and Hornsby, 2018).

In addition, the P2P-IoET project, through a workshop on regulatory and policy pathways to facilitate the deployment of peer-to-peer energy trading through distributed ledger technologies with UK and French industries, policy communities and academics, indicated that trusted local actors...
can become key intermediaries between energy consumers and market actors (Schneiders et al., 2018). Such intermediaries can defend the interests of consumers by involving communities in developing and applying rules on the use of IoT platforms. Thus, these industry developments can facilitate the establishment of more dynamic mechanisms to ensure cybersecurity and consumer protection.

Furthermore, the SGP Stream investigated the role of technical epistemic communities such as Computer Security Incident Response Teams (CSIRTs) or Anti-Abuse Working Groups (e.g. M3AAWG) in maintaining the resilience of the internet’s infrastructure in the face of growing misuse of insecure IoT devices in cyberattacks such as Mirai or Hajime. Our research identified that CSIRTs play a growing role in supporting science diplomacy in cybersecurity and, through active collaboration and joint incident responses, contribute to the adaptive governance of cybersecurity risk (Tanczer et al., 2018d). The SGP Stream has also collaborated with Stanford University on the use of cybersecurity reputation mechanisms established in anti-abuse communities to support formal standards development, as a means to shortcut time-consuming standards review processes while maintaining their consensus-based and transparency requirements (Brass and Sowell, 2018).

Lastly, together with our partners in the WEF, and the NIPC project, we developed a paper on the global governance of IoT security, looking at innovation in this space from other sectors and integrating work from the WEF on ‘agile governance’ (Lesniewska and Carr, in preparation). Here we considered the IoT as a new global critical infrastructure upon which various processes, practices and functions will increasingly rely.

CONCLUSION

Research carried out by the SGP Stream and the PETRAS projects featured in this chapter has extensively examined the positive and negative implications of IoT (in)security, at the device and ecosystem level. Our research has highlighted the need to better align existing and emerging regulatory frameworks for data protection, safety, security product and service liability (RF3). We have also identified the need to create more coherent technopolitical coordination at the international level through the development of standards and more adaptive modes of governance. Our investigation uncovered a marketplace for data that brings new benefits but also new risks to consumers, operators and managers of critical infrastructure and insurers. These developments suggest that, like the Internet, the IoT is gradually becoming the global critical technology platform or infrastructure on which new businesses, products and services flourish. This trajectory highlights the mounting importance of security, privacy and trust in this new converging environment of connected objects, infrastructures and ubiquitous services. The progressive phenomenon of convergence is likely to render existing sector-specific regulations incompatible, thus requiring more flexible and dynamic ways of setting and adapting domestic policies and international coordination practices.

The ability of objects to sense and communicate in an ever interdependent IoT ecosystem expands the scope and scale of threats across all IoT components, challenging existing risk assessment practices and the traditional approach to implementing consent (RF1). This requires continuous efforts to advance understanding and assessment of risks in the complex IoT environment. While the PEDASI Demonstrator successfully developed a data provenance system, providing a technical solution for the absence of transparency and traceability in data handling, more work is required on the issue of data protection to ensure consumer trust. This includes evaluating the
effectiveness of data protection legislation and cultivating new norms that make the connection among activities that generate data, data use and implications of such use apparent to individuals. Given the gap in cybersecurity training and skills development identified by the SGP Stream in the UK and beyond (RF2), further systematic efforts are needed to improve IoT literacy across all sectors of society to ensure effective security and data protection. Such efforts contribute to addressing social problems, such as technology-facilitated crime and exclusion, in terms of prevention, response, support and resilience building. They also look at trust in IoT and facilitate data trade. Despite the currently fragmented landscape (RF3), standards serve as promising operational tools for translating policy and regulatory principles into technical and design specifications, as well as organisational risk assessment and governance frameworks. Standards are expected to play a significant role in building trust in IoT and ensuring trustworthiness across IoT application areas. This means there should be continuous work in standards development.

The future challenges for IoT standards, governance and policies will derive from progressive convergence at the technology, industry and market level, as new cross-sectoral and cross-stakeholder alliances and business models emerge. Convergence at the technology and market level are already observed in cross-sector product and service provision, as in the case of smart car manufacturers' entrance into the insurance market (DDIP-IoT project). However, intensifying convergence across these levels could also lead to new market reconfigurations that would require us to rethink how we measure dominant positions and assess our current antitrust laws. As observed in Net Neutrality policies, the dilemma in regulating convergence manifests in three dimensions: functionality, principles and politics (Pothong, 2018). In an advanced IoT ecosystem, the functional dilemma will likely stem from the close interdependence between the internet infrastructure, communication networks, data markets and edge services. For the second dimension (principles), we are already seeing competing policy priorities, regulatory objectives and frameworks of previously distinct market sectors. The political dimension will involve difficulties in aligning principles for standards, governance and policies across these market sectors and national borders, requiring closer cooperation at transnational and international levels.
REFERENCES


Industry and research organisations have to address the security and assurance of systems incorporating AI and Machine Learning, as well as maximising the use of such techniques in designing resilient systems. Important work driving Security by Design principles already has traction. However, further work is needed to take account of the specific nature of cyber-physical systems. Over 30 years of human factors / ergonomics research in related safety-aware industries such as aviation has led to the development of Security Ergonomics by Design – which considers how security is designed into the development of safe and secure cyber-physical systems and can be used in the context of IoT. There are still no robust tools and techniques to effectively audit emerging safety and security threats in IoT. The traditional security audit procedures are not compatible with most IoT integrated critical infrastructure systems. There is a need to apply the economics of security and trust to the development of protective and resilience mechanisms to increase the cost to the attackers, and to make it difficult to profit from compromising the systems. Further work is required on the development of comprehensive simulation and testbed systems to understand the behaviour of complex cyber-physical systems. Current simulation systems are fragmented because they work at discrete layers of the IoT systems, e.g. physical, software, network, application, logical, etc.
STANDARDS, GOVERNANCE AND POLICY
SAFETY AND SECURITY
PRIVACY AND TRUST
HARNESSING ECONOMIC VALUE
ADOPTION AND ACCEPTABILITY

Cyber Risk Assessment for Coupled Systems (CRACS)
Blockchain-empowered Infrastructure for IoT (BlockIT)
The Internet of Every Things (P2P-IoET)
Blockchain Technology for IoT in Intelligent Transportation Systems (B-IoT)
Analytical Lenses for IoT Threats (ALIoTT)
IoT in Control (IoTinControl)
Industrial IoT (IioT)
Newcastle Urban Sciences Building IoT (NUSBioT)
Security Risk Assessment of IoT Environments with Attack Graph Models (SECRIS)
Impact Assessment Model for the IoT (IAM)
Designing Dynamic Insurance Policies using IoT (DDIP-IoT)
Geographic Personal Data and Location Based Services (GeoSec)
Security and New Threats in Healthcare (SeNTH)
Security and New Threats in Healthcare+ (SeNTH+)
Potential Impact of IoT Boosted Botnet Attacks (BotThings)
Securing IoT in Critical National Infrastructure (SecCNIoT)
SAFETY AND SECURITY
Razvan Nicolescu, Barnaby Craggs, Emil Lupu, Awais Rashid

INTRODUCTION

The main objectives of the Safety and Security Stream were to understand the current and emerging challenges in IoT systems from a safety and security perspective. The challenges ranged from those raised by small implantable sensors in healthcare to those in emerging complex ecosystems such as Smart Buildings or Critical National Infrastructure. In developing and operating efficient IoT systems that are able to scale and support a variety of network and end services, we are challenged not only to understand and manage complex systems, but also to grasp the changing nature of safety and security.

The key finding of the Security and Safety Stream work is the promotion of Security Ergonomics by Design that prioritises safety and security in cyber-physical systems such as the IoT (Craggs and Rashid, 2017). Security Ergonomics by Design goes beyond Security by Default and Privacy by Design and usable security, which set out broad design principles in their respective domains. Security Ergonomics by Design considers how security and privacy are handled by the device across its lifetime and possible varying contexts of use. This concept belongs to a wider recommendation to adopt and practise an evolutionary perspective in relation to safety and security.

A second key finding of our Stream is represented by the need for dynamic assessment of safety and security. In a smart building scenario, these terms can mean very different things for a human operator, a user of or a visitor to the building, and these meanings can vary in time in ways that are not so well understood at present. Therefore, potential compromises to systems of the building need to be assessed in a dynamic way. Not only are there different perspectives but the system itself evolves – the occupancy of the building evolves, new sensors are added, new bring-your-own devices (BYOD) are added that interact with the building’s systems and the use of the building itself brings changes to the overall system.

In this context, we need to perform continuous risk assessment in order to cope with the dynamic nature of IoT. This can be extended to other security aspects. For example, there is a need for continuous authentication through biometrics or from patterns of usage, e.g. keyboard, screen swipe use or driving behaviour.

In IoT systems, the dynamics of the system, the number of devices, cyber-physical integration and the size of the supply chains result in a large surface of attacks. Even with appropriate changes in managing this attack surface, it will become increasingly difficult if not impossible to avoid system compromise. As a result, it is likely that we will need to be able to continue to operate with systems that have been partially compromised and this requires a continuously evolving security and safety culture and improved skills.

In this context, a further major finding is the need to address seriously emerging cultures of security and enforce codes of conduct in the safety and security space. Cultures of security are changing but the pace and depth of this process are rather uneven. We need dedicated resources to drive cultural changes in relation to safety and security for the new IoT systems.

Another major finding is the need to study the emerging security economics and trust economies. For example, possibilities to monetise the compromise of new cyber-physical and cloud systems have to be not only explored and understood, but also potentially used to prevent or counter-attack crime. The systematic use of compromise detection systems can significantly increase attack costs as it forces attackers to trade off between impact and detectability. The economic
aspects around safety and security must include consumer issues and procurement questions for the government.

The UK Government has recently formulated concerns about the needed digital skills (DCMS, 2016). We need to enhance the practical knowledge of IoT challenges for undergraduates and postgraduates. This should be reflected in dedicated changes in the curriculum in disciplines such as computer science and engineering, with specific modules for skills development. Practical assignments should be extended and a whole set of national data challenges in this area is proposed.

**BACKGROUND WORK**

The work in the Safety and Security Stream started from the following fundamental premises:

1) We need to understand human factors (HF) in complex systems in order to advance safety and security in environments, products and services. Our work showed that latent design conditions lead to human errors and we need to adopt principles of security ergonomics to address this issue. Rather than just highlighting 'user error' we should build on the large body of work on usable security that highlights the causes that underpin these errors.

2) Safety and Security in IoT challenges many of the conventional HF premises (Hawkins, 1987; Reason, 1990, 2008; Shappel and Wiegmann, 2000), as IoT can mean multiple environments, different kinds of humans and different parts of a system of systems. In this context, predicting human action is not a reasonable task, especially due to the number of organisational, cultural and environmental factors. For example, in Industrial Control Systems (ICS), the operator’s perception of risk can be unknown, leading to operational mistakes and active errors (Frey et al., 2016).

3) We need to address complex route cause analysis by translating tools such as the Human Factors Analysis and Classification System (HFACS) during the entire lifetime of the IoT systems – design, development, operations, maintenance, end-of-life and recycling (Shappel and Wiegmann, 2000).

4) Security risk assessment in IoT needs to consider the information flows and the dynamic processes that happen within the IoT system of systems.

5) Safety increases with usability and user awareness training, so we need processes to increase usability and user awareness of the new IoT systems.

**INSIGHTS AND FUTURE RESEARCH AGENDA**

Based on findings from the work carried out by Safety and Security Stream as well as relevant PETRAS projects, we advance the following recommendations and suggested directions for future research.

**Continuous Risk Assessment in Order to Cope with Dynamic Change**

The evolving, contextual and dynamic nature of the IoT systems, the diversification of supply chains and of the markets requires that processes previously considered as static checkpoints should be performed on a continuous basis. For example, authentication should not only be conducted when a user starts using a device or when the device is first connected to the system, but a continuous authentication process should ensure that the user and the device remain the same throughout the entire operation. Authorisations based on physical parameters such as location, which can change, should be continuously re-evaluated.

Risk assessment to the different parts of the system needs to be performed continuously as the system, the threats it faces and the degree of compromise can vary in time. This is exacerbated in integrated systems, such as the electricity grid, which diversify from a small number of suppliers to distributed ‘prosumer’ networks. Impact assessment of compromise, risk mitigation strategies and resilience should be considered on an ongoing basis and follow the dynamics and evolution of the system,
the threats and the compromises. This process will require reconsideration of the guidance, standards, regulation and safeguards put in place, although the extent to which each of these must be revised will depend on the sector characteristics and systems considered. In many cases we do not have the technology and methods to enable continuous risk assessment and this fact should inform and drive the research agenda.

Need to Evolve towards Security Ergonomics by Design

There is a need for safety and security to be implemented from the design phase and for the possible future evolution of the system. Important work driving Security by Design principles already has traction, however further work is needed to take account of the very particular nature of cyber-physical systems and over 30 years of human factors/ergonomics (HF/E) work in related safety-aware industries such as aviation. To design secure and safe systems we need to employ well developed and mature methodology to capture and transform design processes. Security Ergonomics by Design builds upon prior design principles and encapsulates HF/E into the design of safe and secure cyber-physical systems (Craggs and Rashid, 2017).

Security Ergonomics by Design completes regulatory requirements and recommendations for basic system design such as Security by Design and Privacy by Design in order (1) to ensure their consistency in requirements and complementarity; (2) to facilitate compliance from manufacturers and operators; and (3) to give users clear expectations about the products and services they use.

Continuously Evolving Security and Safety Culture

We need to address the emerging cultures of security and enforce codes of conduct in the safety and security space. Cultural aspects have influence over the design, development and usage of cyber-physical systems, and in some cases can actually be responsible for their failure. Within Security Ergonomics by Design, there is a need for a ‘Just Culture’ which affords safe space to identify and explore failure with the explicit intent to inform systems design. Errors in the design and operation of cyber-physical systems can thus be reported without an automatic presumption of blame, as otherwise it is all too easy for security problems to go undocumented and unaddressed within complex systems.

These efforts involve engaging with personnel on topics of security and the IoT, as well as performing tasks for continuous risk assessment at different levels. These actions should be translated into standards and take regulatory form.

This recommendation addresses consumer aspects and cultural questions and also procurement questions for the government. We need dedicated resources to drive cultural changes in relation to safety and security for the new IoT systems and to make this process more inclusive and fairly distributed across populations.

Industry has to Address Emerging Threats in Ever Larger Attack Surfaces

The ability of IoT systems to sense and act upon the physical world should be augmented with the capability to interpret the data and react autonomously to changes. These mechanisms are fundamental in the next generation of design of attack detection systems and management of attack surfaces. They

---

1 Since the publication of Security Ergonomics by Design, the principle of Just Culture (Reason, 1998) has been prepended.
2 This challenge was clearly found in the CRACS project (see Nurse et al., 2018).
3 The audit of cybersecurity skills training and awareness programmes developed by the UK Government conducted by the SGP Stream is a good starting point.
include the possibility to continue to operate with systems that have been partially compromised.

Therefore, the industry should find solutions to cope with emerging threats ranging from tampering with devices to threats related to AI and big data. These solutions should start from the fundamental role of data analytics and AI in interpreting change, managing the systems and enabling values to be generated when systems continuously evolve and change. One important aspect is the use of AI and big data to ensure systems resilience. AI methods also bring their own vulnerabilities that should be considered and mitigated in systems design and deployment.

Need to Understand the Risks Related to IoT in Critical Infrastructure

Most IoT-integrated critical infrastructure systems are unable to withstand traditional security audit procedures, thus making it impracticable to undertake security studies and analysis on real systems and platforms. We need to understand the emerging safety and security threats and develop analysis tools and techniques to respond to the needs of security management in the IoT-integrated infrastructure domain.

Better Understand the Risks Related to and Applications of Blockchain Technology and Smart Contracts

We have to understand what risks blockchain technologies and smart contracts enable and when/ in what conditions these risks are suitable. A related issue is looking exclusively at the technical risks around these technologies and ignoring the fact that many operational blockchains are not truly decentralised and can fail to account for humans who require trust, at the most basic level, to adopt and use such technology. The risks presented to individuals should be thoroughly assessed by policymakers before the technology is made available to consumers for everyday use.

Need for Integrated Simulation and Modelling

This recommendation is the requirement for a framework to ignite development of simulation systems to improve safety and security of entire complex systems, rather than safety and security of specific subsystems or aspects. This requirement includes impact analysis, sensitivity analysis to system changes and resilience of the systems, including even when they have been partially compromised.

Further Research in Trustworthiness

We need a way to standardise credibility, including in software and in hardware. Safety is essentially related to trustworthiness and practices around safety and security. However, trustworthiness in IoT systems is an emerging property that is not well understood. For example, we need to set clear expectations of trustworthiness for end user systems, find ways to characterise these expectations and benchmark IoT products in relation to them. We should then agree on the underlying principles of this process at a global level.

Understand the Economic Aspects around the Dynamics of Security and Trust Economies

One key economic aspect related to the dynamics of security and trust economies is to understand the mechanisms of monetisation in order to characterise and defend against emerging threats. Further research into the evolution of threat and the relation to crime and monetisation is needed.

Secondly, we need to understand how to respond to mechanisms that seek to monetise the compromise of IoT systems. We need to focus on protective mechanisms that increase the cost to the attacker and make it difficult to profit from compromising the systems. This principle should lead the efforts to design attack detection systems to block or harness criminal practices.
The economic aspects around safety and security must include consumer aspects and procurement questions for the government.

**Broader Focus on Societal Aspects Related to IoT**

There is a burgeoning need for policymakers and systems designers to more fully engage with wider audiences to understand the acceptable (and unacceptable) aspects of the IoT, particularly in relation to safety and security. For example, blockchains are suggested to afford a route for enhanced security but are consumers accepting of information placed on the chain being immutable? For policymakers this goes further into understanding how such immutability is compatible with legislation such as GDPR and the right to be forgotten.

We need dedicated resources to drive change in relation to safety and security for the new IoT systems. For example, we can start by understanding what is acceptable for IoT consumers. Policymakers should employ qualitative research methods to explore these issues with consumers, industry and the public sector.

**Dedicated Training and Education**

We need to enhance the practical knowledge of IoT challenges for undergraduates and postgraduates. This should be reflected in dedicated changes in the curriculum in disciplines such as computer science and engineering, with specific modules for skills development, but also extend practical assignments and a whole set of national data challenges in this area should be proposed. The Newcastle Smart IoT System lecture course provides a good example.

**Standards and Frameworks**

1. We need to guide the development of simulation systems to improve standards. Current simulation systems are fragmented also because they work at discrete layers of the IoT systems, e.g. physical, software, network, application, logical, etc.

2. We need a way to score vulnerability for IoT devices and systems. A guide to the reliability of the IoT device can be provided after assessment. For example, IoT devices can be purchased and then tested in customers’ own environments and with their own requirements and then a sort of score be applied. This can be done if we define standards that vendors should respect. So, a score would be computed in relation to the compliance to these standards and vendors would know if their products are considered safe by the different communities. In the absence of such a benchmark mechanism, it is challenging to make devices really secure.

3. Policymakers should involve consumers more in their processes and ask questions about what is acceptable for consumers in terms of guiding the development of standards.
CROSS-CUTTING THEMES/ASPECTS

Safety and Security Stream worked with a series of PETRAS projects to address the current technical and societal challenges related to safety and security of IoT. Nine areas of research focus (RF) have been identified.

RF1: Blockchain Technology

This cross-cutting theme has the goal to increase the security of IoT infrastructure through the use of blockchains. Blockchains can help with decentralisation, improve data integrity and auditability of the behaviour of networked systems. But there are also challenges in terms of scalability to wide networks that use IoT applications in complex settings. For example, the choice of blockchain technology to be used in an IoT application is highly dependent on the consensus protocol used and on the scalability properties.

Blockchain as a distributed database and/or computing platform may have privacy issues, since by definition blockchain is a distributed ledger, which replicates data and computation on all network nodes. Moreover, according to the consensus algorithm employed, there can be problems of security, which can hinder consistency or availability.

The BlockIT project at Southampton University addressed the trade-offs between scalability, security and performance in blockchain infrastructures for IoT-based smart energy (see Box 2.1). Specifically, BlockIT aims to define a blockchain-based infrastructure to enable energy trading among prosumers, i.e. nodes in the grid that act both as producer and consumer. To trade the energy the idea is to employ smart contracts on top of the blockchain so transactions in the grid can be verified by everyone. While blockchains do not scale easily, IoT networks have a high number of nodes with different functionalities that are meant to scale. The project focused on the types of consensus protocols that can be used in blockchain networks in order to respond to specific requirements regarding trade-off between consistency and availability. The problem can be illustrated by Figure 2.1.

**FIGURE 2.1** The question is which consensus is needed for blockchain in order to address a particular trade-off between these parameters (BlockIT at Southampton).
The BlockIT project uses blockchain technology to build smart contracts (SC) integrated with smart meters in the smart energy environment. This infrastructure will enable consumers to find the policy they need and trade energy with other members in certain conditions. For example, customers can set rules to buy energy only when their battery is lower than a certain percentage, but buy maximum 1MWh and pay less than a certain amount. This is done through an auction enabled via SCs on the blockchain. Individual and business energy providers can participate in such auctions and trade energy.

This architecture is built on three layers. The first layer enables this policy through SC. The second layer enables energy trading between users on the blockchain. The third layer is a security layer. It represents a knowledge base where essential security information is kept, such as the updated versions of the firmware for all the smart meter devices in the network. For example, when one device is not updated, you can isolate that device from the network using a consensus mechanism. This would allow the update or maintenance to be done and then the device would rejoin the network. This is not a direct way to enforce security, but is a way to mitigate attacks that would exploit known firmware vulnerabilities.

The UCL Energy Institute project ‘The Internet of Energy Things: Supporting Peer-to-Peer (P2P) Energy Trading and Demand Side Management through Distributed Ledger Technologies such as Blockchain’ (P2P-IoET) looks into whether peer-to-peer energy trading can take place on the energy grid as it is currently regulated. The grid is heavily regulated due to its status as critical national infrastructure (Schneiders and Shipworth, 2018). Blockchain technology cannot fully prevent potential irregularities from taking place in the system. Smart contracts can mitigate misbehaviour by coding promises (expectations) into clear contracts (for deliverable goods). However, in this context, blockchain technology is used more to automate the transaction process. This does not address one of the biggest problems in the sector, which is the tampering with IoT devices. For example, if an attacker is able to attack the smart meter firmware, they can get malicious access into the network. Therefore, one further research question the project is asking is about the vulnerability of the grid when consumers start trading energy between one another.
The Blockchain Technology for IoT in Intelligent Transportation Systems (B-IoT) project developed at Imperial College, together with XAIN, a Universal Access Control system for smart vehicles. Different service providers (such as car insurers or DHL deliveries) have the possibility to access different records or sections of the vehicle under specific conditions using blockchain architecture. This solution also offers increased security for vehicle software that is used for flexible access transactions and for secure update opportunities. The project also developed a way to significantly reduce the high energy consumption for mining in blockchain applications with practical adaptation of existing technology used in the automotive sector (Lundbaek, 2018a, 2018b).

RF2: Threats

There is a constant evolution of threat that IoT businesses and operators should be aware of and work to address. However, most IoT-integrated critical infrastructure systems are unable to withstand traditional security audit procedures. This makes security management a challenge as it is unclear how and to what extent existing security threats and analysis tools and techniques can be effective or impactful on an IoT-integrated infrastructure domain.

The Analytical Lenses for IoT Threats (ALIoTT) project at UCL explores the range of security modelling, design and analysis tools, techniques, approaches and supporting policies that might be envisaged to assist in identifying and addressing security and trustworthiness in the systems that use IoT. The project explores these security lenses in relation to critical infrastructure protection tools and techniques (Watson and Ani, forthcoming-b) and Open Source Simulators for ICS/IoT (Watson and Ani, forthcoming-a), and underscores their capabilities for interdependency, resilience and security risk modelling and simulations. The project is also investigating design considerations to assist in establishing or improving credibility of ICS security testbeds for security studies.

The IoT in Control (IoTinControl) project explored the vulnerabilities that exist in industrial (PLC and SCADA) and building control (BMS) systems. The project also considers cybersecurity architectures that deliver the necessary consilience of security and safety policies. It is producing an analytical review of protection approaches in critical infrastructure (Watson and Ani, forthcoming-b).

In smart buildings, security should not be considered solely at the design stage, but rather throughout their entire lifecycle. The Newcastle Urban Sciences Building IoT (NUSBiIoT) project delivered by Prof. Carsten Maple and Hugh Boyes (University of Warwick), Dr Charles Morisset and Dr John Mace (Newcastle University) and Tony Williams (Cube2 Ltd) proposed a multi-modelling proof of concept for assessing IoT security in a Smart Building scenario. They used the integrated toolchain INTO-CPS to model and assess security of smart buildings. The project resulted in a set of recommendations that are illustrated in the case study in Box 2.2.

---

4 https://medium.com/next-level-german-engineering/the-porsche-xain-vehicle-blockchain-network-a-technical-overview-e1148c3c9e73d
5 NUSBiIoT was delivered by Prof. Carsten Maple and Hugh Boyes (University of Warwick), Dr Charles Morisset and Dr John Mace (Newcastle University) and Tony Williams (Cube2 Ltd)
6 http://into-cps.org/
2.2

SMART BUILDINGS

The Newcastle Urban Sciences Building IoT project focused on the cybersecurity of smart buildings using the £58m Urban Sciences Building (USB) as a case study. The USB has been designed as a living laboratory and comes with a wide range of networked sensors and data collecting devices. The high connectivity of smart buildings like the USB exposes their building management systems (BMSs) and other automated systems to multiple cyber-based threats. To investigate these threats, the project team conducted the following.

1. A security assessment of the BMS and building systems to locate potential vulnerabilities and backdoors that may allow unauthorised access to manipulate the building systems and data.

2. A proof of concept multi-modelling study of building systems to support the integrated analysis of their emerging security and safety properties.

The security assessment’s findings led to a list of key recommendations that could help develop a new risk assessment process for similar environments to the USB.

- It does not matter if a building is secure or not until something of ‘value’ is placed within it. The definition of ‘value’ must be reviewed and thought of from different viewpoints, whilst the item of value must itself be reviewed to ascertain where its worth lies.
- A cross-disciplinary security group should be developed to oversee research projects conducted in living labs and review procedures. It is imperative that continual monitoring of research projects is performed in case additional measures become necessary to maintain overall building security.
- Review the ease with which people can generally access and move around a building without being challenged. In particular, when any maintenance is carried out in a building, a signed agreement known as a Permit to Work should be issued stating exactly what work is to be done, where and when. The maintenance work should be stringently assessed by building management at each stage, especially in areas critical to building operations.
- Different locks and keys are required for each plant room which houses mechanical and electrical equipment operating essential building services. Inside each plant room, the

PROJECT NAME
Newcastle Urban Sciences Building IoT (NUSBiT)

TEAM
Carsten Maple (University of Warwick), Hugh Boyes (University of Warwick), John Mace (University of Warwick, seconded to Newcastle University), Charles Morisset (Newcastle University), John Fitzgerald (Newcastle University) and Tony Williams (Cube2 Ltd)

PARTNERS
Newcastle University and Cube2 Ltd
RF3: Risk Assessment

Several projects in the Safety and Security Stream worked on aspects of cyber risk assessment. The Security Risk Assessment of IoT Environments with Attack Graph Models (SECRIS) project at Imperial College proposed mechanisms to perform continuous risk assessment in dynamic environments (such as IoT infrastructure). They provided the tools to do risk assessment automatically and at a fine rate of granularity. The project worked on Bayesian attack graphs that allow probabilities to be automatically computed through various algorithmic approaches. It developed a method and algorithms that enable dynamic analysis in scenarios of multi-step attack spreading through the system (Muñoz-Gonzáles et al., 2017). These mechanisms advance the efficiency of Bayesian inference on attack graphs in IoT environments and scale them up to thousands of nodes. Dynamic analysis consists in continuously revising the risk estimate to different parts of the system in light of evidence of compromise generated by Security Information and Event Management (SIEM) software and forensic investigation of its components. This allows a continuous estimate of the risk to different parts of the system and to select and prioritise the most appropriate countermeasures. This represents an important development in continuous security risk assessment in IoT infrastructure.

The Cyber Risk Assessment for Coupled Systems (CRACS) project at Oxford adopted a more theory-driven approach to identify four key situations where traditional risk assessments fail to adequately define and characterise cyber risk in IoT (Nurse et al., 2017). For example, current risk assessments methods are periodic (instead of dynamic) and assume complete knowledge about a system. In IoT however, data change very quickly and the system is extremely dynamic; this makes attaining complete system knowledge impossible and renders bi-annual risk assessments quickly outdated. Even the range of harms that can result from cyber-attacks is much larger than before (Agrafiotis et al., 2018). These challenges were explored and validated in the
WE NEED TO MOVE FROM STATIC RISK ASSESSMENT TO DYNAMIC RISK ASSESSMENT. WE HAVE TO LOOK AT HOW METHODS FOR VALUE RISK ASSESSMENT CAN BE ADAPTED TO CAPTURE THE DYNAMIC NATURE OF IOT SYSTEMS.

Various approaches to risk assessment for IoT are being developed, based on the economic impact of IoT technologies, physical security and the relation between cyber, physical and other elements of the specific application areas and the risk assessment as well as liability models used in the insurance sector.

RISK ASSESSMENT BASED ON SCENARIOS THAT ARE CONSTANTLY REVISED AND UPDATED TO KEEP UP WITH THE CHANGES IN SAFETY AND SECURITY.

The context of focus groups and interviews with security professionals (Nurse et al., 2018). As a result, the project investigated a set of enhancements to traditional risk assessments, developing two scenarios where dynamic risk assessment for IoT would be important: smart factories/smart manufacturing and smart health/smart hospitals. They helped to examine how the more dynamic assessment approach would work in practice.

The IAM and DDIP-IoT project worked on understanding the economic impact assessment for IoT cyber risk. For example, the IAM project proposed an efficient way to quantify IoT risk, developing the IoT MicroMort model that integrates established risk assessment approaches with existing cyber risk assessment frameworks and represents a much needed quantification tool for calculating the economic impact (Radanliev et al., 2018a). In particular, the IoT MicroMort model adapts to IoT both the Cyber Value at Risk model, an established model for measuring the maximum possible loss over a given time period, and the MicroMort model, a widely used model for predicting uncertainty through units of mortality risk. This work resulted in a series of recommendations for performing cyber risk assessment for IoT and better understanding the economic impact of this technology (Radanliev et al., 2018b).

The project NusBIOT at Newcastle and Warwick proposed a risk assessment framework for smart buildings that includes methodology and a set of proposed actions and recommendations for undertaking risk assessment in a smart building. This included a real-world risk assessment done on the science building in Newcastle that focuses on physical security and the relation between cyber, physical and other elements of a smart building. The second task was to find ways to model systems in the building, see how different elements of the building can be modelled using different languages, build a management system and run simulations. The project also assessed the responsibility for security and safety. One of the main results of the project is that in smart buildings security risks are unclear to owners, users at different managerial level and service providers. Security is not considered at the design stage and it should be. These types of findings were also identified in the CRACS project, but from a more theoretical perspective (Nurse et al., 2017).

The SGP Stream identified the insurance sector as a potential instrument to address and mitigate emerging some aspects of IoT risks. However, the current insurance sector needs to make substantial efforts to address the emerging issues in IoT complex systems and systems of systems. The DDIP-IoT project is partially addressing these issues by working together with Lloyd’s Registry Foundation to develop a framework and formal models to create and manage policies for cyber insurances based on IoT data. This work should be considered in conjunction with the current efforts in cyber risk assessment.
HEALTHCARE

The projects SENTH and SENTH+ (complemented by work from the stream researchers) worked on autonomous security in healthcare using miniaturised devices where computational resources are limited and on-node processing and energy-aware and energy-harvesting techniques are highly demanded. The project also investigated fail-safe mechanisms for reliable sensing and data integrity.

For example, one question the project asked was how we can use the physiological requirements to improve security in pairing sensor devices (key management). This operation is severely restricted in a healthcare environment, where there are important limitations imposed by the physical (small-scale devices, healthcare environment), human (e.g. patients and medical staff) and cyber (e.g. limited computational resources) aspects of the system.

One strand of the work looked at how physiological factors such as arterial blood pressure and Interpulse Interval (IPI) can be used to perform secure sensor association or association between an external reader/programmer and an implanted device. The Physiological Value Based Security (PVS) schemes allow wearable and implanted devices to communicate with one another, as long as they can measure the same underlying physiological signal. The project showed how an arterial blood pressure signal could be used to improve the usability of PVS schemes (Turner et al., 2018). The work showed that raw IPI and EEG signals are weak sources of randomness, but in an important breakthrough it designed novel ways to extract sufficient randomness from these signals to create temporary cryptographic keys to start secure communication (Chizari et al., 2018).

Another strand of the work focused on gait analysis, proposing to improve the security of existing biometric cryptosystems (BCS) by using a new lightweight symmetric key generation scheme based on the timing information of gait extracted from body sensors (Sun et al., 2017). As most of the wearable and implantable devices are embedded with inertial sensors capable of capturing gait signals, the proposed method could enable secured communications between these devices without any additional sensor or hardware. The method also addressed the issue of variation in sensor placements. An artificial neural network framework was developed to estimate lower limb attitude with foot-worn inertia sensors (Sun et al., 2018). The framework was then integrated into the BCS to improve the robustness of the gait-based biometric scheme (Sun and Lo, 2018). Inertial sensors can be used to generate random numbers to secure the communication link among wearable and implantable devices. Based on this concept, a new inertial sensor based random number generator is proposed, and its ability to generate random numbers was demonstrated (Sun and Lo, 2018b).
RF5: Simulation and Modelling

The ALIoTT project explored the possibilities of enhancing reliability of an IoT system used in critical infrastructure using simulation. They looked at simulators for the physical network as well as vulnerability assessment tools for IoT. The project wants to provide a single framework to guide the IoT community and identify a consolidated recommendation for simulation. In particular, the project assesses the use and utility of Open Source simulators (e.g. NS-2, SCADASim and OMNET++) for security modelling and analysis in industrial control systems (ICS) and the Industrial Internet of Things (IIoT), and investigates where there are gaps in the systems that need improvement. One key conclusion is that no single Open Source simulator sufficiently meets the complex needs of connected cyber-physical systems, so capabilities of existing simulators have to be aggregated. There is also a need to explore if generic simulators can expand their capacities into multi-class domains, supporting easier and faster modelling of complex systems (Watson and Ani, forthcoming-b).

The lack of integrated simulation tools means that the impact of malicious attacks upon IoT systems cannot be easily studied and understood for risk management and resilience. At the same time, results from alternative systems design or alternative risk mitigation strategies cannot be easily compared. There is currently no agreed framework to assess trustworthiness and reliability across IoT systems. Results depend on the different aspects people want to simulate and the goals they want to achieve in the IoT space, which are not always very clear. For example, in terms of safety and security, each IoT player performs their own simulation, developing testbeds and running assessments. Even connecting and integrating simulation tools is not straightforward, as these tools may use different models, different assumptions and are programmed in different languages. This can represent a challenge when systems engineers run simulation in conjunction with testbeds, such as in the case of hardware-in-the-loop simulation. There are other aspects related to differences in terms of what is widely accepted, Open Source licence types, operating system platforms and compatibilities, user interfaces, available documentation and types, and system architecture. These conditions lead to inefficient use of resources and long time to market.

RF6: Liability and Responsibility

Whilst liability for cybersecurity events remains a poorly understood yet critical area, we are acutely aware that the very process of ascribing liability for security events may lead to undesirable behaviours when it comes to reporting and learning from incidents. Even regulatory efforts such as those enshrined in the GDPR (calling for reporting of problems before causation has been determined) may have unintended consequences upon security as the tensions between corporate responsibilities play out. In this context, more thoughtful ‘Just Cultures’, as embedded in Security Ergonomics by Design, would afford a safe space to identify and explore failure with the intent to inform both systems design and the setup of liability boundaries.

Security represents a common good, when a system can be compromised to attack its data and functionality but also when a system is used as stepping stone to compromise the security of others, e.g. in botnet attacks. A further key aspect is related to the liability chain for devices and systems. Across the different sectors and IoT systems there is an issue of how much liability should the manufacturers, intermediaries, retailers and end users bear and for what. It is unclear what measures and processes should be put in place to ensure that the owners of the liability can make informed decisions and which risks can actually be insured. For example, currently there is not sufficient liability for software flaws. The role of technical communities is not always clear or regulated, e.g. the current changes in corporate social responsibility will probably make pre-sentence investigation reports more important. However, more work should be done to fully understand the emerging landscape.
In a smart building scenario, security responsibility is complex. It requires awareness and integration of different domains such as building knowledge, documentation and management that is distributed across a series of personnel, organisations and stakeholders, rather than centralised in, and limited to, a building management centre. The NUSBiIoT project demonstrated how multi-modelling can be used to assess security of CPS/IoT. The project also revealed the continual hurdles when assessing buildings, such as access to documents and cultural barriers. Contracts and non-disclosure agreements can be complex and lengthy and can lead to important delays.

Domestic abuse can be exacerbated through IoT. The Gender and IoT (G-IoT) project at UCL explored the possibilities to mitigate domestic abuse and proposed to focus on the abuse facilitated by consumer devices in domestic environments and against vulnerable communities (Tanczer et al., 2018a, 2018b). This is an instance of using IoT to mitigate and ensure the security and safety of the physical space.

As reasonably controlled markets, for example, supply of electricity, become more decentralised and the production becomes more democratised, new regulatory challenges emerge. For example, decentralisation in the energy grid raises numerous questions for policymakers regarding the status of ‘prosumers’, network charges, data density and ownership (P2P-IoET project). In this context, smaller providers are relatively more vulnerable and they have less capability to protect themselves. Some may be malicious. The resilience of the resulting systems needs to be understood, and regulation must ensure this resilience whilst facilitating access to market. One consequence is that regulators need to formulate new terms for liability in the energy sector.

Distributed data attacks and botnets cross international boundaries, so policies can become complex and liability becomes unenforceable. From a social perspective, when people wear personal devices that attack others, they might have a sense of social responsibility and they should be supported by the larger community in solving possible problems. We need to understand when and in what context it is important for a state to intervene and through which means.

It is important to place liability in a specific context. For example, in domestic contexts, IoT liability is with the device owner, while in medical devices liability is more tightly controlled. Regulation on sale can apply to both and supply chains extend beyond national borders, but safety considerations mean that medical devices are more tightly controlled. However, little is currently understood about the inherent risks of connected medical devices and consequently standards and regulation are lacking.
RF7: Possibility to Monetise the Compromise of Physical and Cloud Systems

In IoT cyber criminals can resort to complex extortion schemes. There is a question of what to attack and how to monetise these attacks. Cyber criminals currently try to make money either via services (third parties) or remote access to the attacked user. Monetisation is done through DDoS and Remote Access Trojans (RAT). Criminals can steal personal data or records, but this requires compromising the back-end where all the computation takes place. There are possibilities of new attacks in the supply chains, e.g. Trojan horses, because of data theft or hijack. This context requires further work with industry on the possibilities to implement and offer secure services.

The Modelling the Potential Impact of IoT Boosted Botnet Attacks (BotThings) project at UCL provides guidelines for the National Cyber Crime Unit on how to deal with malware at the UK level – what the threats are and what they can do about it. The project has two objectives: understand the existing malware and find solutions for mitigation and identifying potential threats. They proposed measures for IoT botnet mitigation: better default configurations (including passwords) and better mechanisms for automatic updates. This work should inform the secure by default code of practice.

The EVIoT project developed a framework for supply chain integration in an IoT-enabled supply chain network (Wakenshaw et al., 2017). The analysis identified a key concern associated with information sharing in the supply chain between secure environments and more primitive and unsecure environments. The key issues are how the cost of the security solutions and their benefits can be balanced out with the risks for the deployment of IoT systems in the supply chain network.
The GeoSec project explored the limits of computational privacy in mobile networks – threats and recommendations for standardisation. For example, one important aspect that you cannot stop in the mobility sector is location-based attacks. So, the project explores mechanisms to secure mobility services, for example, through signing and verifying safety messages. It proposes to increase security and reliability by using advanced methods for verification that are suitable in a mobile environment, e.g. low energy consumption and relatively small overheads.

In energy trading, there is an issue of vulnerability of integrated systems like the electricity grid to: (a) compromise of a large number of devices e.g. many identical smart meters by the same malware; and (b) prosumers that may not be able to protect their systems.

RF8: Consumer Aspects

It is agreed that social aspects should lead technical advancements around safety and security. For example, trust is fundamental. Consumers would not use an IoT system if they did not trust it. This includes, but is not limited to, whether consumers feel safe to use an IoT system. Policymakers focus on security in relation to data. However, more effort should be made around further consumer aspects, such as acquiring digital skills and addressing cultural questions.

We need trade-offs between technical and social aspects in different contexts. The needs for safety and security can be different across populations and geographical contexts. For example, the P2P-IoET project looks at the social and regulatory barriers to the deployment of peer-to-peer energy trading in the UK energy sector. The issue of consumers’ engagement with the technology is central to the project. In order to test this, a game simulating peer-to-peer energy trading was designed, which gives consumers an idea of how P2P energy trading using blockchain would work. Furthermore, a national survey of energy consumers was conducted, testing their views on different aspects of peer-to-peer energy trading such as its locality and governance framework, as well as their perceptions of blockchain technology (Schneiders et al., forthcoming). The aim is to produce recommendations for policymakers and industry stakeholders.

RF9: Standards

There is a fragmented standard landscape that needs harmonisation. The SGP Stream looks at how IoT standards are developing and the current issues related to governance.7

---

7 See Chapter 1 of this report.
IOT IN CRITICAL NATIONAL INFRASTRUCTURE

The Securing IoT in Critical National Infrastructure (SecCNIoT) demonstrator looks to the evolving concerns around the use of IoT within safety critical industrial control system (ICS) operational environments. Traditionally these sites have relied upon physical security and a lack of connection to the internet for their cybersecurity, however with the adoption and convergence of IoT, and more recently industrial internet of things (IIoT), there are growing concerns that operational environments may be exposed to new threats deriving from the IoT.

The demonstrator builds upon the Bristol Cyber Security Group’s ICS and IoT testbeds to undertake three core tasks. First, it highlights the anatomy of attacks within this converged environment, and principally within a water treatment plant testbed. There are known weaknesses in both the equipment and protocols used by industrialised IoT and where these are placed onto and into ICS environments it is plausible that those weaknesses can be exploited to attack the operational ICS equipment itself. Secondly, the demonstrator looks to enhanced risk analysis for such converged environments based upon work by Cardiff and Imperial College. This work brings forth the areas of the ICS/IoT environment which are most vulnerable, and the impact of them being attacked on interdependent components, so that there might be more targeted mitigation to secure vulnerable areas. The third and final part of the demonstrator looks to industrial partners to validate this approach to risk identification and mitigation within other industry verticals.

Together this demonstration seeks to help those tasked with the running of critical national infrastructure take advantage of the benefits of IoT/IIoT in more timely, cost effective monitoring and control of operational environments, whilst better understanding the risks presented by this emerging technology space.
CONCLUSION

Security for cyber-physical systems is hard. Making the IoT both safe and secure is a challenge that presents as wicked and will take the combined resources of multiple academic disciplines, government agencies, device manufacturers and the public themselves. We will never be able to secure everything, protect against all forms of human error let alone all threats. However, sensible design practices, sound methodological practice for understanding failures of safety and security (be they deliberate or inadvertent) and a willingness to continually review risk within such complex converged systems provides some light at the end of the tunnel.

IoT is and remains a fast-moving landscape. The IoT systems are dynamic, with the emerging of new devices, technology, e.g. blockchains and smart contracts, new adoption and value-creating models. Threats vary too. The geo-political context is constantly shifting, as are ways in which criminals can take advantage and profit from systems. In this context, it is important to consider the security and safety of IoT not only as a set of tasks but also as a continuous process and a changing landscape.

The socio-technical aspects of IoT are complex. They include consumer trust, vulnerability of systems to cyber-threats, as well as the use of IoT for a safer and more secure society. However, these aspects cannot be considered without addressing trade-offs between privacy and monitoring, between time to market and adequate consideration of security and safety.

In this context, there is much commonality across sectors, such as healthcare, transportation, energy and manufacturing in terms of the changes that IoT introduces and which we should be increasingly aware of. However, the threats, risks, impact and the way in which these aspects need to be mitigated vary across sectors, as do the intervention mechanisms and the degree of contextualisation. Therefore, there is a strong imperative to establish continuously evolving security and safety culture and improved skills.
REFERENCES


Developers should consider using various privacy assurance approaches to enhance user-perceived control of their data in the provision of their IoT services.

Privacy policies often fail to communicate clearly the risks of data processing and linkage of user records.

Privacy assurance approaches include individual self-protection through privacy policies as well as technical features, industry self-regulation and government regulation.

Links between IoT objects and services can inadvertently contribute to discriminatory profiling.

Developers should increase information transparency in the IoT systems through interfaces between the systems and the users, taking into account socio-technical intersection and cultural diversity.
STANDARDS, GOVERNANCE AND POLICY
SAFETY AND SECURITY
PRIVACY AND TRUST
HARNESSING ECONOMIC VALUE
ADOPTION AND ACCEPTABILITY

Blockchain Technology for IoT in Intelligent Transport Systems (B-IoT)
Displays and Sensors on Smart Campuses (DiSSC)
Data Analysis in IoT Solutions for Healthcare (DASH)
Respectful Things in Private Spaces (ReTiPS)
Displays and Sensors on Smart Campuses (DiSSC – Campus)
Smart Transactions in Public Spaces (STIPS)
Trust and Privacy as Design Principles for IoT Infrastructures (DePrIoT)
Blockchain Technology for IoT in Intelligent Transport Systems (B-IoT)
Privacy and Trust in Connected and Autonomous Cars and Smart Transport (P-Cars)
Privacy-Enhancing and Identification Enabling of IoT Solutions (PEIESI)
INTRODUCTION

Privacy and trust are clearly two vital components of a successful Internet of Things (IoT). Privacy has been prominent in the news lately, with the General Data Protection Regulation becoming law to protect the rights of citizens. Without trust, there will be a limited acceptance of IoT by government, industry and citizens. There is a requirement that systems can be trusted and IoT can be used without breaching privacy. Early in the PETRAS project, the researchers in Privacy and Trust (P&T) Stream identified the gaps in the current research literature regarding privacy and trust in the IoT, from a social and a technical perspective. The meta-analysis of the social science and humanities research on privacy and trust in IoT identified the wide-ranging primary ethical issues: control and oversight on data flows; the balance between authentication and privacy; criteria to foster users’ trust in IoT; trade-offs between identification and privacy; the limits of the GDPR; transparency and auditing of autonomous and machine learning algorithms; responsible innovation; and consent mechanisms.

The technical issues we identified include:
- trustworthy systems;
- meaningful consent mechanisms for IoT;
- subjects’ control of their data;
- anonymity models for data management in IoT;
- computation on encrypted data (homomorphic encryption);
- localisation and tracking;
- profiling and user privacy requirement;
- public presentation and privacy;
- lifecycle transition and data transparency; and
- unlinkability and linkage.

Recently, we revisited our meta-analysis through a workshop with researchers of the PETRAS hub. Many of the issues that we identified in our gap analysis were reiterated. In this chapter we focus on three major themes in which advances have been made in the PETRAS project. These are:
- Trustworthiness and Control
- Transparency and Consent
- Privacy by Design

These issues have been addressed through what we term constellation projects as well as part of the core P&T Stream work (see Appendix 1 for details). Here we describe and discuss the work undertaken. It is important to recognise that the impact of the hub research extends beyond what is reported here, both in scope and depth, but we aim to present the diversity and reach of the work.

INSIGHTS

Based on the outcome of PETRAS projects and the stream work, we have identified high-priority areas and make the following recommendations for different actors in the IoT ecosystem.

Privacy Assurance Approaches

In the privacy literature, control has been a key factor for privacy protection. Xu et al. (2012) argued that, in addition to technical capability to control the information display (Zweig and Webster, 2012) based on individual choices, control could be achieved through industry regulation and government regulation. In IoT, subjects’ control of data and the corresponding data flows was identified as one of the key issues initially identified for privacy and trust research. Developers should consider using various privacy assurance approaches – individual
self-protection through privacy policies and technical features, industry self-regulation and government regulation – to enhance user perceived control of their data in the provision of their IoT services. However, privacy policies often fail to communicate clearly the risks of data processing and linkage of user records. Following the GDPR (Articles 5 and 25), IoT developers and providers should define new standards relating to informed consent, notification duties, privacy by design and privacy by default, data protection impact assessment, algorithmic transparency, automated decision-making and profiling.

Privacy Profiling

Measures should also be taken with respect to profiling. The collected data and monitoring facilitate the creation of profiles that lead to inferences and predictions about users. Sensor fusion (linking datasets from different devices) provides ever more detailed insight about users’ private lives, enabling assumptions about and predictions of their behaviour. Linkage between IoT objects and services can inadvertently contribute to discriminatory profiling. Third parties with whom the data are shared (insurance companies, employers and police) can use the data in combination with their own datasets for purposes not intended when the data were collected or consented to by the user. Such linkage is problematic since IoT systems are built on the idea of connectivity and data sharing, hence these risks are intrinsic to IoT systems. To minimise these risks, developers and providers of IoT technologies should guarantee users control over their data.

Information Transparency

Information transparency is crucial for users’ perceived control and privacy protection. It entails ‘customer knowledge of a firm’s access to her or his data and understanding of how it is going to be used’ (Awad and Krishnan, 2006, p. 42). This could be achieved and communicated with customers via privacy policies. Information transparency is also described as a facilitator of knowledge (Schauer, 2011, p. 1343), ‘the principle of enabling the public to gain information about the operations and structures of a given entity’ (Etzioni, 2010, p. 1). In order to enhance transparency, the information provided has to be ‘fair, reliable, complete, consistent and presented in clear and simple terms’ (Etzioni, 2010, p. 11). The developers should increase information transparency in the IoT system through the interfaces between the system and the users. Interfacing should consider socio-technical intersections and cultural diversity.

RF1: TRUSTWORTHINESS AND CONTROL

The first major research focus (RF) that drove the work of the P&T Stream centred around the issue of trustworthiness, trust and control.

Issue 1: Trustworthiness

Trustworthiness was identified as one of the key issues for privacy and trust research in the initial workshop. First, from a technical point of view, trust negotiation (the exchange of credentials that allow a requesting party and servicing party to deliver a service or resource) is key for the development of a trustworthy system. This negotiation requires identity management and access control. Any trust negotiation mechanisms developed in the IoT must have appropriate access control and ensure that the mechanism is fine-grained but not burdensome, especially since adequate object identity management systems, to record the identity of objects and their authentication, authorisation, roles and privileges, are not yet developed. Technically, trustworthiness is contextual: it needs to be addressed in a context and should be goal oriented. Different variables need to be considered for different contexts.

Second, in the workshop discussion, it was emphasised that trust issues could cut across several areas. For example, we have to address trust in complex environments/interchange points across business initiatives. We need to ensure that there is trust throughout the supply chain, in the sense that a stakeholder, wherever they may sit, needs some trust
in all those involved in the chain. In IoT contexts this is challenging, as there are multiple service providers, multiple devices and distributed control. Complexity goes further than production supply chains. Consider the case of driving in a connected and autonomous vehicle from Edinburgh (our most northern partner in PETRAS) to Southampton (our most southern). During that journey, a passenger or driver will interact with numerous services, operating through numerous architectures, delivered by numerous operators. For them to have trust in the objective (to travel from Edinburgh to Southampton) requires direct and indirect, explicit and implicit, trust in the system.

Third, while the characteristics of trustworthy systems (reputation/past performance, resilience, safety, security, reliability and availability) are necessary, they remain insufficient to assess a system's trustworthiness from a user's perspective. Indeed, fostering user trust in IoT was identified as a key issue that requires ethical and social understanding. Trust intersects users' experience but also grows when users' rights are respected and when transparency, for example over data flows, is guaranteed. Research has shown that information transparency through privacy policies can increase user trust in organisation information activities (Martin et al., 2017). Users’ trust also rests on the reputation of the providers of the service and the resilience of the technology.

**Issue 2: Control**

First, control has been investigated in the PETRAS project from technical perspective. In a system, access control is a crucial element in achieving trustworthiness. The need to exercise access control is recognised (Maple, 2017). The access control could be over ‘the Internet of things at the edge of the network in the device, or at least, a local access controller for the device (Cerf, 2015)’ (Maple, 2017, p. 168). The issue has been considered alongside the related issues of identification/authentication. Secondly, control also needs to be addressed as a psychological issue. For example, Xu et al. (2012) showed that perceived control over personal information is a key factor affecting information privacy concerns. Subjects’ control of their data and data flows has been identified by the team as one of the key issues that requires further work. Privacy concerns can be affected by privacy assurance approaches such as individual control (enhanced by privacy policies and privacy enhancing technologies), industry self-regulation and government legislation (such as GDPR) (Xu et al., 2012). Research has shown that perceived control (even if this control is not manifested) for an individual can increase user trust towards service provider. Many projects have addressed this issue. For example, for personal data, technically the shift from centralised systems to decentralised systems regarding data and data analytics can give users more control.

From an ethical and social perspective, control counterbalances trust. Trust implies reduced control from the trustor's side. Trust also entails the delegation of a task to a third party, without controlling how the task is executed (Taddeo, 2010, 2017). Translating this into IoT scenarios has unveiled a number of crucial issues concerning data flows and who oversees data collection, sharing and storing. At the same time, issues have surfaced concerning the design of IoT technologies to enhance user control and capabilities to control smart, IoT, environments, without encroaching upon users' self-determination.

Various issues associated with trustworthiness, trust and control have been investigated by researchers in PETRAS hub. The issues investigated include: contextual trustworthiness from technical perspective; development of trustworthy systems through enhancing adaptive access control; user control in public space; and overriding control in healthcare. Some of this work is presented in this chapter.
3.1

CONTEXTUAL TRUSTWORTHINESS

Current and future vehicles are being developed to utilise V2X (vehicle to everything) communications for a variety of safety, driving efficiency and infotainment applications. For example, vehicles use V2X communication technology to periodically communicate status information, such as position, speed, heading and acceleration, to surrounding vehicles and infrastructures. Vehicles can also be informed of traffic information such as accidents, approaching emergency vehicles and weather conditions. Such situational awareness will help avoid collisions and reduce fatalities and serious injuries as well as having an environmental impact. Since vehicles and infrastructure form ad-hoc networks for communications, it is important that this communication takes place in a trusted environment. The work in the P-Cars project involved the development of an algorithm that combined group signatures for privacy (discussed later in this chapter) and event linkability, based upon short-term linkability. While long-term linkability is a serious issue for privacy, short-term linkability provides an important mechanism to ensure trusted, attributable (even if not in real-time) communication. In this project, the short-term linkability is given in the context of a vehicular event, such as an accident. An event is uniquely identified through the use of a timestamp, a location name, a random number or an incident summary, depending on the use case. A crucial aspect of linkability for preventing Sybil attacks, in which a system is subverted by forged identities, is that the users cannot bypass the linkability on the messages that are supposed to be linked. In our work we propose a framework which formalises anonymity, traceability, event linkability and unforgeability.

MAIN PROJECT OUTPUTS

TRUSTWORTHY SYSTEMS: ADAPTIVE CONTROL AND ACCESS CONTROL

The B-IoT project is an example of a project that considers development of trustworthy Systems – in this case, through adaptive control and access control mechanisms.

B-IoT work includes contributing to a framework for distributed adaptiveness and user control for energy-critical and low-latency platforms such as those used in the mobility sector. B-IoT developed with XAIN AG, in a pilot with Porsche, the first blockchain developed in cars (XAIN, 2018). The new technology allows tracking and safety hashing data while users are in control of the data and supports the dynamics of a majority of nodes that consistently enter or leave the network. At the same time, access control over machine permissions can be assured in real-time and securely. Thus, in this system, the consensus mechanisms, cryptography-based access control, anomaly detection and machine learning of system parameters for run-time adaptation are coordinated and distributed throughout the blockchain network. Such synergistic architectures should provide much more resilient and robust blockchain systems, as they will support self-stabilizing system behaviour that can reflect a variety of features and their trade-offs in an optimal manner.

MAIN PROJECT OUTPUTS


USER CONTROL

In DiSSC, we brought together an emerging large-scale sensor network with the world’s largest experimental pervasive display network to explore the issue of IoT trust in the context of smart campus systems. While the IoT is typically thought of in terms of simple sensors and actuators, pervasive displays (ranging from digital signage through to specialised control panels) form an interesting element of the IoT – offering local storage, processing and display capabilities together with a means for users to interact with the surrounding IoT. This work was the first comprehensive investigation into future IoT ecosystems that feature situated and pervasive displays as trusted portals and mediators for proximate IoT sensing devices. We conducted a set of studies and a focus group exploring user attitudes towards their awareness of IoT sensor deployments both in private (e.g. homes), semi-public (e.g. offices) and public spaces (e.g. libraries or learning zones). The outcomes of these studies revealed a general lack of understanding about the level of IoT-based sensing taking place and the privacy and security implications of the collected and analysed datasets. In addition, we developed and deployed an enhanced privacy-aware display personalisation framework at Lancaster and integrated the framework with the sensing units provided by Surrey, allowing users to dynamically retrieve sensor readings from proximate devices as they walk by displays.

MAIN PROJECT OUTPUTS


OVERRIDING CONTROL

IoT in Healthcare (H-IoT) technologies increasingly play a key role in health management, for purposes including disease prevention, real-time tele-monitoring of patient’s functions, testing of treatments, fitness and well-being monitoring, medication dispensation, and health research data collection. H-IoT promises many benefits for health and healthcare. However, it also raises a host of ethical problems. The project first analysed the main ethical problems that have been identified by the relevant literature and identified key themes in the ongoing debate on ethical problems concerning H-IoT (Mittelstadt, 2017). Users, already in a vulnerable position as patients, face a seemingly impossible task to retain control over their data due to the scale, scope and complexity of systems that create, aggregate and analyse personal health data. To respond to this problem the project developed guidelines for the design of technologically robust and scientifically reliable IoT technologies that would also be trustworthy and respectful of user rights and interests (Mittelstadt, 2017).

The project identified nine ethical principles for the ethical design of H-IoT devices and data protocols:

• Facilitate public health actions and user engagement with research via the H-IoT;
• Non-maleficence and beneficence;
• Respect autonomy and avoid subtle nudging of user behaviour;
• Respect individual privacy;
• Respect group privacy;
• Embed inclusiveness and diversity in design;
• Collect the minimal data required;
• Establish and maintain trust and confidentiality between H-IoT users and providers;
• Ensure data processing protocols are transparent and accountable.

Nine guidelines have also been identified to embed the proposed ethical principles in the design of H-IoT, prior to adoption by users and subsequent assessment of acceptability:

• Ensure data processing protocols are transparent and accountable.
• Establish and maintain trust and confidentiality between H-IoT users and providers.
• Ensure data processing protocols are transparent and accountable.
• Give users control over data collection and transmission;
• Iteratively adhere to industry and research confidentiality standards;
• Design devices and data sharing protocols to protect user privacy by default;
• Use alternative consent mechanisms when sharing H-IoT data;
• Meet professional duties of care and facilitate inclusion of medical professionals in H-IoT mediated care;
• Include robust transparency mechanisms in H-IoT data protocols to grant users oversight over their data;
• Report the uncertain utility of H-IoT data to users at the point of adoption;
• Provide users with practically useful mechanisms to exercise meaningful data access rights;
• Design devices to be unobtrusive according to the needs of specific user groups.

MAIN PROJECT OUTPUTS


### WHAT INFLUENCES PERCEIVED TRUSTWORTHINESS?

People’s perceptions of devices and systems are shaped by a myriad of factors in ways that are not often well-understood. In the ‘Strangers in Your Room’ study, we had participants who were end users of smart home devices unpack what ‘smartness’ of smart home devices means to them. This revealed nine main kinds of functionality in users’ mental models of such devices: supporting apps (**apps**), supporting voice control (**voice**), being connected to the internet (**connected**), supporting remote access and control such as via a smartphone app (**remote control**), supporting autonomous sensing (**sensing**), responding to sensed situations (**responsive**), demonstrating some form of learning based adaptation (**learning**), and supporting the ability to assume tasks on behalf of the user (**delegation**):

<table>
<thead>
<tr>
<th>APPS</th>
<th>CAN INSTALL APPS FROM APP STORE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice Control</td>
<td>Responds to spoken commands</td>
</tr>
<tr>
<td>Connected</td>
<td>Connects to the internet</td>
</tr>
<tr>
<td>Remote Control</td>
<td>Via an app or computer</td>
</tr>
<tr>
<td>Sensing</td>
<td>Knowing what’s going on</td>
</tr>
<tr>
<td>Responsive</td>
<td>Responds to sensing or other stimuli</td>
</tr>
<tr>
<td>Learns</td>
<td>Changes behaviour based on past interactions</td>
</tr>
<tr>
<td>Delegation</td>
<td>Can be given tasks to execute on the user's behalf</td>
</tr>
</tbody>
</table>
Each of these kinds of functionality was associated with concerns that impinged on the ability to trust and fully use these devices. Delegation for instance, was associated with concerns related to autonomy, understood as the ability to make one’s own choices without external influence, or ‘self-governance’. Entrusting tasks to a voice assistant such as Alexa, for example, was seen as potentially restricting one participant’s choice of what to eat for dinner. Similarly, supporting remote control and sensing was seen as entrusting remote access into potentially private spaces, could potentially threaten privacy and affect the social order of such social spaces.

<table>
<thead>
<tr>
<th>TYPE OF SMARTNESS</th>
<th>ETHICAL CONCERN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delegation</td>
<td>Autonomy, Transparency, Uncanny Behaviour</td>
</tr>
<tr>
<td>Learning</td>
<td>Privacy, Transparency, Uncanny Behaviour</td>
</tr>
<tr>
<td>Connectedness</td>
<td>Privacy</td>
</tr>
<tr>
<td>Voice Control</td>
<td>Privacy, Autonomy, Uncanny Behaviour</td>
</tr>
<tr>
<td>Remote Control</td>
<td>Privacy, Autonomy, Social Order</td>
</tr>
<tr>
<td>Sensing &amp; Responding</td>
<td>Privacy, Autonomy, transparency, Social Order</td>
</tr>
<tr>
<td>Apps</td>
<td>Privacy</td>
</tr>
</tbody>
</table>

MAIN PROJECT OUTPUTS


RF2: TRANSPARENCY AND CONSENT

Issue 1: Transparency

Transparency quickly emerged as a theme that was important for privacy and trust in the IoT but had not sufficiently been investigated. From social aspects, the focus is on awareness of privacy and trust in relation to IoT transparency. Information privacy could be an attribute of the organisation in terms of their data management practices. The firm could make the process transparent through disclosing information. Information transparency is defined as ‘customer knowledge of a firm’s access to his/her data and understanding of how it is going to be used’ (Awad and Krishnan, 2006) (Martin et al., 2017, p. 42). Transparency is defined as ‘the principle of enabling the public to gain information about the operations and structures of a given entity’ (Etzioni, 2010, p. 1). Thus, for information or processes to be transparent, the entity should make the information/process available and accessible for examination and scrutiny (Schauer, 2011). In order to enhance transparency, the information provided has to be ‘fair, reliable, timely, complete, consistent and presented in clear and simple terms’ (Etzioni, 2010, p. 11). Indeed, research has shown that information transparency can improve users’ trust.

There is a need to examine how to improve data transparency from the users’ perspective and how it could impact trust. This discussion feeds back into the more foundational questions concerning transparency – transparency of what and to whom? For example, transparency of data processing may be relevant to users, whereas a transparency over informational architecture may be less relevant to the average user, but more central for an engineer working on a given IoT artefact or a third party considering insuring the artefact. Technically, it is important to develop the adaptive interface to present the information for users at the appropriate time. In terms of information apparencty, user capability building and B2C communication need to be emphasised.

Issue 2: Consent and Meaningful Consent

User consent concerns acquiring the required level of permission from users and non-users (Perera et al., 2015). Users have limited time and technological knowledge for giving consent, receiving feedback and interacting with service and technology providers (Perera et al., 2015). Maple described that ‘Consent has traditionally been based on a system of transparency: a provider of a service should make clear what data is collected and what it is to be used for’ (2017, p. 174). User consent is a key mechanism for managing privacy protection and allowing authorised access to information.

Gaining active, informed consent within IoT systems presents a significant challenge. In order to give people informational power, consent has to be meaningful, i.e. consent has to be intelligible to, controllable by and visible to users (Baarslag et al., 2016). It is argued that in order to have meaningful consent, we must move towards an ‘apparencty and semantic/pragmatic transparency’ model in terms of data management: ‘apparencty reflects how an activity is signalled. Semantic transparency addresses whether we know what the terms of the apparent activity (data activity) are and mean; pragmatic transparency reflects the degree to which we know what these data actions actually do or entail’ (Gomer et al., 2017).

Apparencty and semantic/pragmatic transparency models are crucial for meaningful consent.

In order to have meaningful consent in the IoT, we need to understand (1) how to make data activity more apparent; (2) how to make users understand and be aware of the risks and implications of these activities and what their consent means/entails; (3) how to make the terms more readable, understandable, usable and accessible; and (4) due
to the scale and speed of data actions in IoT, how to make the consent automated but also give end users real choices and power of negotiation of consent terms.

The issues investigated include: information transparency from a user perspective; information transparency in IoT from a technical perspective; and meaningful consent in IoT.

3.6 STREAM
Privacy and Trust

INFORMATION TRANSPARENCY

Information transparency can enhance users’ control and foster users’ trust towards service providers (Martin et al., 2017). The stream work centres on how information transparency through privacy policies and technical features can affect users’ trust and control and their willingness to engage in data sharing or other forms of information activities. Research on information transparency has primarily focused on privacy policies (Martin et al., 2017) and centres on the knowledge and understanding of data management processes. However, with technological advancement, the transparency of data management processes can be increased. There exists an (in)congruence between expected and perceived information transparency and this is likely to affect the willingness of consumers to share their information for personalisation.

MAIN PROJECT OUTPUTS


The DiSSC project investigated the interplay between environment information collected through the IoT Egg multi-sensor suite and exploitation of the collected data through use on public displays. The IoT Egg collects a range of environment metrics including temperature, humidity, presence, movement, light intensity, noise levels and dust concentration. The data are for fixed locations and stored in a database, which then is accessed through the display servers and projected to public screens. The user influences the display content through their preference settings, and the display is activated when the mobile app (Tacita) detects the presence of a participating display. The signalling in this case is implemented in a passive way: rather than the user/their application identifying themselves when they approach a display, the display announces itself (via Bluetooth beacons). Using this approach, the user (or app) has to actively use the location identifier (i.e. the Bluetooth MAC address, which is registered with the content server) to trigger the display of personalised content, therefore keeping control of their location information.

MAIN PROJECT OUTPUTS

TRANSPARENCY IN IOT

The STiPS project explored customer responses to the display of real-time provenance data as part of the process of coffee consumption, through the use of the Bitbarista. The Bitbarista is a hacked home coffee machine, augmented with a Raspberry Pi connected to the internet and with its own Bitcoin wallet. It sells coffee and a vote for future coffee supply in exchange for Bitcoin. The aim of the design was to create a sense of transparency around value produced in supply chains and product pricing by offering customers greater insight and involvement. The Bitbarista displays data on coffee-producing countries that it purportedly browses on the web and uses this to derive top-ranked coffees in four categories for its future supply of beans, and the price customers pay for their coffee is based on the future supply they vote for. The STiPS project explored customers’ responses to this process in a study of initial perceptions with 14 participants (Pschetz et al., 2017), and a one-month trial involving a further 13 participants (Tallyn et al., 2018). The study of initial perceptions showed this transparency was welcomed, giving customers a greater sense of trust in the machine. Whilst this was also true for the participants in the longer term study, where this transparency led to their perception of Bitbarista as an ethical machine, we also found difficulties in maintaining customer engagement with this process. Speed of transaction (get me a coffee now) may trump reflection on the process (how ethical is this process I’m buying into?) and there is a need to carefully construct such interventions to fit with people’s daily behaviours and routines.

MAIN PROJECT OUTPUTS


The implementation of the apparency-pragmatic/semantic transparency model is crucial for achieving meaningful consent in IoT systems. First, for apparency, we need to understand how the user interacts with the entities in the IoT system. This could be achieved through mapping scenarios of IoT interactions, exploring the five ‘W’s of who, where, when, what and why data flow across multiple systems and between devices. In order to implement the notion of pragmatic transparency, we need to model users’ understanding about these systems and the associated risks and the options. This could be achieved through

1) identifying the potential threats imposed by the smart devices, such as identity threats, access threats and disclosure threats;

2) understanding threats and risk to the IoT system and to privacy if attacks take place.

In order to enhance semantic transparency, we could develop an ontology to represent the terms used by different groups and to make the consent terms more understandable, usable and accessible. We used the smart home as an example. We believe that the implementation of the model would enable us to develop a framework for meaningful consent for smart devices in a more generic IoT environment (Wakenshaw et al., 2018).

MAIN PROJECT OUTPUTS

RF3: PRIVACY BY DESIGN

Privacy by design is another key issue that was identified in the early work of PETRAS P&T Stream. In IoT, the challenges for privacy include user consent and this leads to another challenge: data management. In IoT, when sensitive data are transferred and deployed into the cloud, how to achieve data protection is a key challenge. How could data be protected by the cloud service provider during (1) transmission; (2) processing; and (3) storing in cloud? In all cases, data must only flow to authorised parties (Singh et al., 2016). In the PETRAS hub, researchers have developed a number of novel methods for ensuring privacy in IoT. One example is the use of the blockchain concept in the project of B-IoT. The framework proposed by B-IoT (XAIN, 2018) enables a privacy-friendly blockchain technology architecture that respects the Privacy by Design principles and is GDPR compliant. (See Box 3.10.)

Moreover, given technological advancements, the provision of real-time, dynamic and in-demand data has increased dramatically. Personalised products and services can generate revenue for firms and enhance their competitive advantage in the market. Yet consumer concern regarding privacy is still the key factor impacting on willingness to share personal information for personalised services and products. Users who express concerns over their own privacy are likely less willing to share such information (Stone et al., 1983) in the online setting (Awad and Krishnan, 2006). It is crucial to develop an understanding of, and to develop socio-technical solutions to reduce, consumer privacy concerns.

During the early P&T Stream workshop, the debate placed a focus on the different cultural traditions that underpin our understanding and regulation of privacy worldwide. For example, the European approach to privacy rests on its relation to human dignity, while the US approach links it to freedom of speech. The discussion then shifted to the GDPR and need to understand how the competing principles underpinning IoT design and technology and GDPR data protection laws could be reconciled and implemented. From the users’ perspective, the relevance of education was stressed as a key element to enhance data literacy and their understanding of privacy. The lack of user awareness would likely result in a lack of trust and privacy concerns; in turn, these may hinder IoT-based innovation. Privacy issues in new technology such as blockchains and smart contracts need to be addressed in terms of their legal implications.

With the launch of GDPR, DePrIoT projects examined the trade-off between the need of IoT technologies to identify and reidentify customers (e.g. in order to tailor services or interact successfully with them) while protecting their privacy. They concluded that, in order to minimise the privacy impact of the conflicts between data protection principles and identification in the IoT, GDPR standards urgently require further specification and implementation into the design and deployment of IoT technologies (Wachter, 2018).
MULTI-PARTY PRIVACY IN IOT PRIVACY IN BLOCKCHAIN

The framework proposed by B-IoT (XAIN, 2018) enables a privacy-friendly blockchain technology architecture that respects the Privacy by Design principles and is GDPR compliant. Only a hash of data is stored on the blockchain, which gives important privacy benefits: mere possession of a hash gives no knowledge of the data that has been added by the originator. This mechanism also assures further important privacy instruments, such as the possibility to update data, to share data between users by re-encrypting the data to allow access, and export data to another service via proxy re-encryption. Due to the fact that IoT covers various application scenarios, the privacy requirements for B-IoT transportation scenario need to be further compatible with other scenarios. Cross-domain privacy among heterogeneous vehicular communication networks is treated as the research focus. Blockchain will help to shuffle pseudonyms among the entire decentralised vehicular communication network, maintaining internal privacy.

Privacy among vehicles is achieved by using pseudonyms to hide their real identity. As the required number of pseudonyms in vehicular communication systems is large, privacy management should take efficiency into account. Pseudonym reuse and exchange are considered as feasible ways to solve the problem. However, it is inefficient for a central manager to arrange pseudonym exchange. With the help of the blockchain, a decentralised management can be realised. Moreover, blockchain assists to share information among nodes and enables all the participants to propose a plan of how to reuse the pseudonyms.

MAIN PROJECT OUTPUTS


3.11

PROJECT NAME
Privacy and Trust in Connected and Autonomous Cars and Smart Transport (P-Cars)

TEAM
Mehrdad Dianati (Surrey), Carsten Maple (Warwick), Jia Liu (Surrey)

PARTNERS
Ordinance Survey; Pinsent Masons; Thales; TRL

PRIVACY IN COHORT

The P-Cars project brought together researchers and industry from the legal and technical professions to consider schemes to aid privacy in connected and autonomous vehicles and intelligent transport systems. To provide a level of privacy to vehicle users, the project developed a new system to provide temporal anonymity (or more technically, k-anonymity, where someone cannot be identified beyond belonging to a group of k individuals) for users, together with unlinkability to reduce the probability of identification of routes to tend to zero as the length of journey and number of vehicles interacting increases. Each vehicle has multiple signatures that are unlinkable, thereby ensuring the user’s long-term privacy. The scheme reduces the computing and transmission overheads inherent in traditional group signature schemes, through the reuse of an event-linking token as a self-certified temporary public key for generating signatures to authenticate the subsequent messages. The group signature acts as a certificate for the temporary public key. Since each user can only create one temporary public key for each event, when the event is over, the temporary public key is automatically revoked. To ensure the desired level of privacy, each event has to be updated in an appropriate time frame. We illustrate how to apply our scheme in the vehicular communications by two use cases: intersection management and cooperative awareness messages.
Trust and Privacy as Design Principles in IoT Infrastructures (DePrIoT)

TEAM

Mariarosaria Taddeo, Brent Mittelstadt, Corinne Cath

(University of Oxford)

PRIVACY AND TRUST TRADE-OFF IN IOT

The DePrIoT projects (Floridi and Taddeo, 2016; Mittelstadt et al., 2016; Cath et al., 2017; Taddeo, 2017) highlighted that IoT provides huge opportunities to improve private and public life while promoting business innovation and economic growth. However, the extensive use of increasingly more data (Big Data), the growing reliance on algorithms in automatic communication and processing (including machine learning), as well as the gradual reduction of human oversight over many decisions pose pressing ethical issues of privacy, trust, transparency and responsibility. If these issues are overlooked, underestimated or left unresolved, they risk hindering the innovation and the progress that IoT can bring to society at large and to future generations.

MAIN PROJECT OUTPUTS


The PEIESI project focused on the trade-off between the need of IoT technologies to identify and reidentify customers (e.g. in order to tailor services or interact successfully with them) while protecting their privacy. Striking this balance is not an easy task because of weaknesses in cybersecurity and anonymisation techniques. The EU General Data Protection Regulation (GDPR) may provide essential guidance to achieve a fair balance between the interests of IoT providers and users. Through a review of academic and policy literature, this project analysed the inherent tension between privacy and identifiability in the IoT. It identified four challenges:

1) profiling, inference and discrimination;
2) control and context-sensitive sharing of identity;
3) consent and uncertainty; and
4) honesty, trust and transparency.

The project focused on the extent to which several standards defined in the GDPR will provide meaningful protection for privacy and control over identity for users of IoT. It concluded that, in order to minimise the privacy impact of the conflicts between data protection principles and identification in the IoT, GDPR standards urgently require further specification and implementation into the design and deployment of IoT technologies (Wachter, 2018).

MAIN PROJECT OUTPUTS


Wachter, S. 2018. GDPR and the Internet of Things: Guidelines to Protect Users’ Identity and Privacy.
Homes are the most private spaces in people’s lives, and thus privacy by design is both a critical and tremendously challenging acceptability barrier for home IoT. However, the rapid adoption of home IoT devices has started to reveal that privacy is not the only perceived concern such devices raise in this very personal context. A closely related concept to that of privacy we have been investigating relates to the multi-stakeholder nature of these devices: today’s home IoT devices are designed to serve more than one master, and this can create perceptions of untrustworthiness, dishonesty or disloyalty that can undermine not only trust, but overall perceived usefulness. While one ‘master’ might be the end user, another might be the device manufacturer; still others might include platform controller(s) associated with these devices (such as Apple or Google), as well as various third parties including advertisers.

The key distinction from privacy by design is that such concerns might arise not only from privacy violations but from the ways such devices behave. For instance, does Amazon’s Alexa virtual assistant respond to requests from users always prioritising the user’s needs genuinely and entirely? Or, does Alexa respond in a way that strikes a balance between the user’s needs and those of Amazon? What other functions do smart speakers such as the Echo Dot do in service of the platform instead of the user’s needs?

Respect by Design goes beyond Privacy by Design, focusing on whether the behaviour of IoT devices aligns with users’ needs.

In our work, we argue for a need to expand the vocabulary with which we can discuss and characterise the behaviours of IoT devices to identify where such behaviours align with, are orthogonal to and conflict with user needs. Drawing from moral philosophy and economics, the aforementioned multi-stakeholder problem is known as a type of moral hazard (Pauly, 1968). Moral behaviour, in a Kantian sense, is behaviour that necessarily treats the other (in this case, end users) with respect. Respect, in turn, means and addressing their needs genuinely, fully and exclusively, rather than as a means to serve one’s own selfish needs. Privacy by Design might be seen as a subset of what we might call ‘Respect by Design’, because any design features that do not address privacy needs would necessarily be seen as not genuinely and exclusively serving the user’s needs, thus not respectful.

Respect by Design is particularly important for the home as that it is not just where the most sensitive and personal interactions occur, but also where users need to be able to trust that IoT devices will always carry out their wishes with their best interests at heart. For instance, shared devices in the home are often used by children, the elderly and the otherwise vulnerable, who have less awareness about how these devices work or when they serve them marketing material. Unfortunately, despite the sensitive contexts such devices occupy, they remain fundamentally driven by surveillance capitalism (Zuboff, 2015), meaning that the manufacturers of these devices see them as a means of furthering their own interests.

In the Respectful Things in Private Spaces ReTiPS project, we have been tasked with exploring what a generation of ‘respectful’ devices might look like, and how they might be developed (commercially or otherwise) and sustained. We have in particular been following a variety of open source, community-driven IoT devices and high-quality smart home IoT devices and software that, due to their being non-commercial, inherently prioritise the needs of users rather than particular commercial entities. In addition, we have begun our own project, Respectful ARETHA, an Alexa-like virtual assistant made of pluggable open source components based around small Linux desktops and micro-platforms. ARETHA represents primarily an experiment to understand the potential of how truly ‘respectful’ virtual assistants that offer assurances may be more suitable than commercial assistants for certain private and sensitive settings.
Beyond Privacy-by-Design for Home IoT: ‘Respect’ by Design?

ARETHA: A ‘Respectful-by-Design’ open-source, moral, virtual assistant

While still under development, ‘out of the box’ ARETHA will support several modes of operation all of which achieve privacy-by-design goals including supporting ‘incognito’ fully forgetful interactions, ‘zero transmission’ interactions in situations where ARETHA can fully fulfil the user’s request without transmitting data to any external entities or third parties, ‘buffered and noisy-channel’ interactions where ARETHA can obscure a user’s identity using cover noise.

Beyond privacy-by-design, ARETHA will also work on behalf of the user to achieve higher standards of respect-by-design goals by serving a user’s needs exclusively rather than in addition to its own, including supporting of selective self-disablement for sensitive situations, and the ability to serve as a network watchdog for all devices in a user’s home.

Figure 3.1 Respectful-by-Design

Main Project Outputs


Mittelstadt, B. 2017. Designing the Health-Related Internet of Things: Ethical Principles and Guidelines. Information, 8(3), 77.

CONCLUSION

The projects and stream work in the PETRAS Hub have addressed many (though not all) gaps identified and reported by the initial state-of-art review and gap analysis, and some new issues emerged. We suggest that the unexplored issues should form our new research agenda.

- **Trustworthy system and trust.** Trustworthy system research in PETRAS was focused on technical aspects such as contextual trustworthiness, adaptive control and access control. However, many other issues, such as how to foster user trust in IoT systems, trust in data and trust across organisations in IoT systems, are still to be addressed.

- **Control.** The control issue has been explored both technically and ethically. User control of their data in IoT was identified as one of the initial key issues for privacy and trust research. Many projects have addressed this issue. For example, the DiSSC project investigated how users can control their data technically in public spaces. The DASH project identified nine ethical principles for the ethical design of IoT devices and data protocols. However, there are many emerging issues – for example, how data management and data analytics in decentralised systems could affect user control and user trust of IoT need to be examined.

- **Information transparency.** This issue was addressed technically within the DiSSC project, which examined IoT labelling, signalling and display of real-time provenance data. Stream work on the other hand looked at information transparency from the user’s perspective. However, many foundational questions remain such as what transparency entails and to whom.

- **Consent.** Consent has been deemed a key measure for privacy protection in current data protection regulation. Stream work has proposed mechanisms for meaningful consent in IoT systems. However, the implementation of meaningful consent mechanisms is very challenging both technically and socially. More research is needed in this area. Moreover, technological advancements such as AI and other data analysis techniques challenge how relevant and meaningful consent can remain as a means for privacy and data protection.

- **Privacy by design.** Research on privacy has centred on technical, social and ethical aspects. Privacy in a cohort, i.e. privacy among multi-parties, was addressed in the context of connected cars. However, the challenge is how to enhance coordination among multiple organisations to address privacy issues in IoT systems. A few other issues need to be addressed including: privacy education; the legal implications of privacy issues in new technology; trade-offs of privacy at the foundational level; market or human rights issues and reconciliation of these issues. While emerging privacy enhancing technologies (PETs) can provide mechanisms to share data privately, recent work undertaken by the Royal Society with input from members of the P&T Stream have found that there are significant challenges in their implementation. At best, widespread effective use of PETs in the IoT is a medium- to long-term ambition.
PRIVACY AND TRUST STREAM: MAIN OUTPUTS


Mittelstadt, B. 2017. Designing the Health-Related Internet of Things: Ethical Principles and Guidelines. Information, 8(3), 77.


REFERENCES


Mittelstadt, B. 2017. Designing the Health-Related Internet of Things: Ethical Principles and Guidelines. Information, 8(3), 77.


XAIN. 2018. Practical Proof of Kernel Work and Distributed Adaptiveness. A Resilient and Scalable Blockchain Platform for Dynamic Low-Energy Networks. Yellow Paper Version 1.2 Available at: https://pdfs.semanticscholar.org/2f1e/cdb469f8540e141917210b2bcbe6243d0a.a.0f8f3a73d3420c6e1170706703.1548691275.pdf [Accessed 10 September 2018].


Standards to address interoperability, safety and security in shared IoT ecosystems are urgently needed to facilitate the creation of economic value, while mitigating the new types of cyber risks.

Although industries are quick to discern what provides the greatest economic value and appropriate IoT data use, the current lack of suitable risk assessment methods makes it difficult to calculate the economic impact of using such data with the desired precision.

Providers of IoT solutions face increased pressure to build solutions that respond to customers’ actual values and expectations and to scale these solutions in order to cover very different, and potentially conflicting, needs.

The industrial sector should identify the beneficiaries of economic value, enable the development and segmentation of new markets and facilitate the promotion and distribution of such value in society.

Integration with critical infrastructure and compatibility with legacy technology represents a key driver for establishing trust and enabling mass IoT adoption.
STANDARDS, GOVERNANCE AND POLICY
SAFETY AND SECURITY
PRIVACY AND TRUST
HARNESSING ECONOMIC VALUE
ADOPTION AND ACCEPTABILITY

The Internet of Energy Things (P2P-IoET)
Economic Value of IoT Data in Cyberphysical Supply Chains (EViIoT)
Value of Personal Data in IoT (VPD)
Smart Transactions in Public Spaces (STiPS)
Impact Assessment model for the IoT (IAM)
Industrial IoT (IIoT)
Smart Road and Street Maintenance, Pricing and Planning (RoadMaPP)
Blockchain Technology for IoT in Intelligent Transportation Systems (B-IoT)
Designing Dynamic Insurance Policies using IoT (DDIP-IoT)
National and International Policy for Critical Infrastructure Cybersecurity (NIPC)
Blockchain-empowered Infrastructure for IoT (BlockIT)
INTRODUCTION

Harnessing economic value in the IoT space is a continuous process. IoT is not simply a consumer technology or a business optimisation tool. Rather, IoT represents an ecosystem of systems that are complementary, interdependent and co-evolving. In this context, harnessing economic value from IoT could be seen as the capacity to create and maintain meaningful IoT ecosystems.

A key objective of the Harnessing Economic Value (HEV) Stream was to identify the economic value of present-day IoT technology and services that typically resides with the owner of data sources (e.g. sensors). This is changing quickly, so we investigated new opportunities to create different sorts of value, including economic value, social values, well-being and local wealth, and to identify where new sectors can emerge, rather than looking at the macroeconomic aspects.

The HEV Stream investigated the long-term economic value that depends on the data becoming a traded and reused commodity in real time and at high frequency, for example, due to Machine to Machine (M2M) automation, with citizen engagement at scale. The importance of HEV aspects of IoT data creates tensions in the design space. A better understanding is needed of complex market design in terms of platforms and ecosystems, institutional constraints such as IP and regulation, data provenance including licensing issues, competition and its incentivisation, and of the ethics and acceptability of data and meta-data sharing.

Another key objective of the HEV Stream was to identify how to get the best out of complex IoT systems, while considering several conflicting objectives, e.g. the overall throughput in urban supply chains and security and privacy of its individual participants. Such optimisations of an IoT system require a solid understanding of how humans would interact with these systems, what the public understanding and acceptance are of different risks and unknown implications, and how design principles can responsibly influence behaviour across populations, e.g. through nudges.

The two objectives relate to each other because the data in IoT systems and systems-of-systems do not have a sole owner and an effective market mechanism is needed for the collecting, sharing and reusing of data. This is vital for guaranteeing the effectiveness and optimisation of IoT systems. For example, market mechanisms need to recognise that consent and control reside with the original purpose of data, avoiding data misuse whilst acknowledging that function creep of data has economic potential. Future cyber insurance mechanisms also must be considered.

The HEV Stream explored emerging business models that consider the value and utility of IoT data and how these change over time, but that also factor in costs such as those for ‘educating’ people on IoT risks and their mitigation. Our work informs the development of a security market, in which security architectures can be designed to be aware of contextual business models and trade-offs between different aspects of PETRAS research hub. We reused and repurposed existing data and considered how this process could be applied in various sectors such as energy and transport. For example, data collected originally for vehicle maintenance regimes can have value for prediction of faults. We looked at the use and adaptation of cryptocurrencies to support not only efficient micro transactions (e.g. to incentivise privacy-preserving sharing of lifestyle data) but also policy-based governance (e.g. to increase overall system performance or marketing efficiency by addressing changes in consumer behaviour). Finally, we produced research papers, model prototypes and case studies that demonstrated the feasibility and utility of market frameworks in the support of efficiency gains in IoT-driven systems.
**LESSONS LEARNED**

Integrating IoT technologies increases cyber risk, which can be visualised by evaluating cyber operational capabilities (Radanliev et al., 2018a). This evaluation in complex systems is different from investigating supply chains and cyber risks on a stand-alone basis. Setting up objectives without visualising and considering digital capabilities would inevitably result in supply chains that have desired but unrealistic cyber security – or recovery planning.

A synergy of social and technical understanding is the best approach for quantifying the impact of cyber risk in the IoT space. The process represents a new design for mapping IoT risk vectors and making the most effective IoT risk impact assessment. The research design identifies and captures the IoT cyber risk vectors and defines the process for adapting existing cyber risk standards to include IoT cyber risk.

We propose a quantification method to assess the economic impact of IoT and its associated cyber risks vectors and vertices (Radanliev et al., 2018a). The HEV Stream adapted well-established models for measuring the maximum possible loss over a given time period, and for predicting uncertainty through units of mortality risk. The new model for calculating IoT risk was tested and validated with real data from over 310,000 scans.

We developed two calculations: the current state of IoT cyber risk and future forecasts of IoT cyber risk. The findings advance the efforts of integrating cyber risk impact assessments and offer a better understanding of the economic impact assessment.

A fundamental finding highlighted the requirement for an interdisciplinary understanding of ‘value’ in the creation of IoT services and products during their entire lifecycle, from design to consumption and retirement or recycling (Nicolescu et al., 2018a). Harnessing economic value from IoT is about balancing out values emerging from three major domains: social, technical and economic.

Value creation cannot be limited to any one domain. Rather, the capacity of IoT systems to generate economic value depends on the skills to trade off concerns within and across the social, technical and economic domains. Unfortunately, interdisciplinary exploration of the meaning of value and value creation in relation to IoT is in its infancy. The HEV Stream analysed domain challenges, cross-domain implications, and proposed a functional model of IoT ecosystems (Figure 4.1).

These learnings and core findings can be structured into ten key challenges and gaps in harnessing economic value from IoT (Nicolescu et al., 2018a, 2018b).

![Figure 4.1 Functional model of IoT ecosystems.](image-url)
1) Lack of Reliable Models for Multi-Modal Values of IoT Systems

We need models that can represent multi-modal values and their interactions to support decision-making. Many IoT applications can create non-monetary value, typically in health and education systems, which could impact key economic values, such as public health spending.

2) Need to Identify Cost Factors/Quantities for IoT Systems’ Lifecycle

The dominance of financial mechanisms for digital technology over more conservative costing models favours technical capabilities over market needs. Many cost factors of design, implementation and operation are unknown or inadequately assessed.

3) Ill-Understood Trade-offs between Technical/Social Capabilities and Economic Costs

Providers of IoT solutions face increased pressure to build solutions that are able to scale and cover very different, and potentially conflicting, needs. There is a growing demand for better modelling and analysis capabilities to support decision-making in this space. Public understanding of technical capabilities, limitations and emerging risks is key for social adoption and for turning economic opportunities into actual business propositions.

4) Better Understanding the Risks and Opportunities of IoT Technology Fragmentation

Harnessing economic value from IoT might be impacted by the existence of multiple competitive IoT ecosystems that could form an increasingly fragmented space in which economic models are likely to be volatile, vendor dependent and less transparent. However, heterogeneity may also offer advantages through competitive innovation.

5) Bridging the Gap between Designs and Actual Implementations

For example, the ITU-T defines an IoT device as ‘a piece of equipment with the mandatory capabilities of communication and optional capabilities of sensing, actuation, data capture, data storage and data processing’ (2012, recommendation Y.2060). But each of these features comes with economic costs that are either unclear or understudied in conjunction to each other and in real implementations.

6) New Risk Assessment Approaches

IoT ecosystems need to include new approaches in relation to structural changes in production and consumption practices. These changes include, for example, rethinking engineering processes, risk engineering assessment throughout the entire lifecycle of the product, reorganisation of labour within organisations and major transformations in the education system and in the professional landscape.

7) Information Models and Semantics

Current data models are insufficient. Semantics-based information models should be an integral part of security, risk management and the design of IoT products and business applications in order to increase the safety and predictability of systems — especially in case of attacks or failures. There is a disturbing lack of data and information management in many IoT architectures, the focus being on the technology and its interconnection rather than system integrity.

8) Current Lack of Interoperability

True interoperability of IoT devices is crucial to maximise value (McKinsey, 2015) and includes the possibility to adopt open standards. Integration with legacy technology and critical infrastructure represents a key driver for establishing trust and enabling mass adoption of IoT.
9) Limited Current Use of IoT Data

The trend to broaden IoT data use from anomaly detection and system control to optimisation currently takes place mostly in the industry sector. This process also involves the assessment and innovation of what provides the greatest economic value (McKinsey, 2015), which is currently not very visible across industrial sectors and virtually unknown to the general public.

10) Fostering Strong Competition, Standardised Interoperability and Open Collaboration

Delays in IoT standardisation and implementation constitute gaps in relation to industry and consumer expectations, but they also represent innovation opportunities. They might allow the organic development and adoption of IoT in different social contexts. Economic models can be volatile, vendor dependent and less transparent. Regulation and policy should mediate conflicts sooner rather than later.

INSIGHTS

Given the challenges we identified, learning from our research and findings from other relevant PETRAS research projects, we advance the following recommendations. Our recommendations aim specifically to facilitate and foster value creation in IoT.

IoT Standards to Support Shared Ecosystems and Services

We have identified an urgent need for standards to support the different verticals that participate in shared ecosystems. Better interoperability of devices and standards that cover several aspects such as safety and security will facilitate the creation of economic value. For example, in the automotive sector there are players in a shared ecosystem that share data and services, e.g. around electric charging services, but they find it challenging to operate in the existing environment characterised by commercial isolation and scale it further. Businesses need IoT standards to enable them to relate to competitors in new ways that should be safe and trustful. Cooperation in this space is the new paradigm.

Timeline: Work on medium to long term.

Adaptive Regulatory Models for New Business Models

Personal data in this domain need a balance between protection by regulation and competition on the market. Users should be made more aware of personal data as currency. Policies and regulations should find ways to enforce equal and democratic access to IoT technology, its by-products and spin-offs across populations, such as in collecting, managing and trading personal data. For example, in areas such as personal data, regulators should leave more space to the market in relation to the extent to which owners of data are in control. These models need mechanisms to implement social and cultural flexibility across communities and populations. Special attention should be given to vulnerable
sections of society and people with lower educational background in terms of fair and ethical access to and exploitation of resources.

**Timeline:** Work should start now and continue.

**Understanding the Distributional Impact of New Business Models**

We need much more work into understanding the ways in which the move from centralised to decentralised systems would impact different populations. Regulatory models should ensure protection of social rights across the entire society. This means industry should be clearer on who is the actual recipient of economic value and how this is distributed in society. For example, privacy sandboxes in FinTech and regulatory sandbox in the electricity sector are shielded ecosystems where people could experiment with the new services. Regulators would not change the system until they were convinced that the new system would not impact negatively some segments of the society. This process should be related to other kinds of regulations, e.g. ISO, in order to align their efforts and reduce hindrance and interference. That could be enabled through more experimental regulations to feed the business models.

**Timeline:** Work should start now and continue.

**Information Apparency and Transparency**

Consumers and businesses should have mechanisms to recognise the relation between activities that generate data and the values of the data they generate, as well as the consequences of that data being used in different ways. IoT industry, government and non-governmental organisations should find ways to build this kind of awareness and capabilities. This would enable a common knowledge that is crucial to the development and operation of IoT. Increased certainty around currently challenging aspects such as total cost of operations in the IoT space, commercial cascading effects, novel liability regimes and privacy law would help increase social trust and adoption of IoT-based products and services. For
example, information appearance can feed new user-centric insurance models. At the same time, there is also the issue of simply making data available vs. making it apparent via a commercial entity. Human agents should be able to make conscious decisions in relation to their personal data. For example, it would be good to find a balance between data transparency and compliance with GDPR.

**Timeline:** Work should start now.

**Understand the ‘Consumer of the Future’**

Disruptive technology should not mean social disruption. We need to understand the unintended consequences of IoT in social and economic terms. The recommendation has a strong research and educational aspect. The work would balance out the bias induced by studying the positive consequences of IoT and would address the current gap in securing the required digital skills. Government actions to improve supply of digital skills have to be resilient against hard to predict technical and economic developments, and ought to include a robust approach to the efficient and fair requalification of the existing workforce.

**Timeline:** Work should start now.

**Insurers are Problematic as ‘Policy Stakeholders’**

Many reinsurance companies face the challenge of using the vast amount of data that is available to create new value-added services. This is a risk in terms of competition as new players start to fill in the gap. The global investment banks were in a similar position maybe ten years ago when new Machine Learning algorithms were introduced. For example, JP Morgan invested in new technology and know-how and they are now ready to compete with any of the big FinTech innovators. In the energy sector this is about the extent to which we are socialising components of costs. Traditionally, with insurers it was not purely risk-reflecting but rather a collective socialisation. In the energy sector there are flat tariffs. Flat tariffs themselves do not reflect social aspects. For example, during the day the retired and the house-bound are cross-subsidising the rich who work. If you change that situation to a cost-reflecting situation you would distribute costs and charges with important social consequences.

**Timeline:** Work should start now.

**KEY CROSS-CUTTING THEMES AND FUTURE RESEARCH AGENDA**

HEV Stream works in collaboration with relevant PETRAS projects to identify and evaluate the main challenges to harnessing economic and value construction for IoT. These challenges manifest in four facets which form our cross-cutting themes and future research focus (RF).

**RF1: Cultural and Organisational**

These capture different values that emerge in IoT-based services and products while giving people the social and cultural values they are habituated to or enjoy, e.g. individuality vs. sociality, autonomy vs. community-focus, or different levels of interest in environmental issues. In terms of harnessing economic value, the cultural and organisational aspects relate to the extent to which we are socialising components of cost and the distributional impact of IoT services. But these aspects also highlight the ways in which we use IoT in order to ensure protection for vulnerable segments of society.

These aspects are explored in different ways in PETRAS research hub.

**IoT can be used in supply chain integration to increase the efficiency of work and reduce costs through resource tracking and integrating lifecycle information in order to connect procurement, quality control, assurance and delivery.**
• The EVIoT project developed a framework for supply chain integration which reflects the importance of organisational culture, including skill sets awareness, objectives and top management commitments at the strategic level (Wakenshaw et al., 2017). While the benefits of IoT applications for supply chains have been relatively well documented, there is an important gap in terms of finding ways to plan together and make and sustain collaborative relationships in IoT-enabled supply chains at the strategic level.

• Another challenge is represented by the attempts to quantify the Value of Personal Data in IoT (VPD) project. The project worked with the case of Hub of All Things (HAT)8 to design and create a personal data platform that would enable the emergence of a primary personal data market (Ng et al., 2017). It conducted a qualitative study that identified the factors affecting whether consumers share their information and a quantitative study that explored how much value consumers would put on several sets of data. It considered emerging questions from both business and consumer perspectives, including: How to make personal data valuable? How to enhance the quality of data? How to capture the cultural value?

• We need further work on understanding social values that emerge from IoT-enabled business models and environmental aspects around consumption. For example, the P2P-IoET project looked at the social values that emerge from peer-to-peer energy trading. The project developed an interactive game model that allows people to implement a peer-to-peer system and actually experience it. It elicited the preferences and intentions of users in order to identify different patterns and ways to use energy. The project looked at the range of social values that emerged and explored how stakeholders can incentivise different options. In particular, this work showed that legal entities such as Limited Liability Partnerships and particularly Co-operative Societies can play a crucial role in providing the necessary framework to protect consumers when using smart contracts and engaging in P2P transactions (Schneiders and Shipworth, 2018).

• In a similar vein the Smart Transactions in Public Spaces (STiPS) project showed that social interactions at a local level can inform and address some of the challenges faced by governments who work at higher levels and have rather limited means to intervene, e.g. through taxation and regulation.

RF2: Creation of New Business Models
This is about identifying areas where value is liberated in order to create the space for new business models. The fact that many of the benefits of IoT have public or quasi-public character, e.g. the benefits of smart transportation and smart city technologies on environmental quality and on public safety, raises considerable challenges for finding business models to finance investments in such technologies. The service models associated with enabling healthier, safer and greener environments in urban and work contexts are still in their infancy. However, when the benefits of IoT are studied in a bottom-up approach, businesses can identify ways in which the general public would be happy to actually pay for smarter services. For example, in some areas, platform businesses have been able to build sustainable business models. These can be highly effective in the context of the emerging Chinese political economy.

E-commerce platforms, such as Alibaba, Baidu and Tencent, are already using personal and transactional data collected to offer personalised and segmented financial products, such as micro-credits and insurance policies.

---
8 https://www.hubofallthings.com
The STiPS project explored the interchange between different kinds of values beyond the conventional economic understandings of value. The project questioned the value propositions in IoT space through a series of design interventions, which are indicative of a multi-sided market.

Bitbarista is a Bitcoin coffee machine designed and built to demonstrate the properties and potential of blockchain and explore perceptions of value transactions with an IoT device. The ethos of the Bitbarista is to create more awareness of the process of consumption and a reported growth in instant self-focused experiences, as opposed to services like AmazonDash or AmazonGo. Bitbarista displays data on the state of coffee-producing countries, looking for information on climate, work conditions, political situation, infrastructure, price stability and demand, which the machine purportedly browses online. In response, clients have an option to consider future supplies based on these data, not just on the taste of the coffee.

The project constructs new business models that have different forms of currency and capital and can offset conventional costs for a coffee service. Bitbarista connects customers more directly with the growers and the circumstances of the product they are paying for. People participating in creating the service find the particular environment enabled by Bitbarista more transparent and meaningful but it can challenge other important social values. For example, one of the findings in the project is that, by using micropayment as an incentive, Bitbarista can undermine social values of cooperation and a sense of giving in a shared environment or community. People might not enjoy being incentivised or paid a small amount to give their time and energy in different social contexts. Several participants in the study reported that the Bitbarista’s micropayments undermined the sense of value in altruistic social contributions. The project reports important variations in the way people attach value to the function of the money.

Bitbarista helps understanding of some of the social consequences of IoT technology in economic, social, cultural and pedagogic aspects. Digitisation of small transactions and too much transparency in the supply chain can create supplementary competition between coffee growers because of higher and less consistent demand for coffee, which is in conflict with its apparent ethical proposition. On the other hand, Bitbarista attempts to move beyond brand, for example in relation to marketing. Instead of conventional marketing products, the quality of the product can be associated with increased clarity about its provenance, a sense of ethical consumption and trust in data.
These aspects are explored in different ways.

- **Industry 4.0 (I4.0)**, commonly referred to as the fourth industrial revolution, is a name given to the current trend of automation and data exchange in manufacturing technologies. It includes cyber-physical systems, the IoT, cloud computing and cognitive computing. The Impact Assessment model for the IoT (IAM) project explored the relation between Industrial IoT (IIoT), I4.0 and the national strategies or initiatives in this space (Radanliev et al., forthcoming-a). The project mapped that current evolution and its associated cyber risks for the I4.0 sector and correlated academic literature with 14 world-leading I4.0 frameworks and initiatives. One important finding is that in many Western countries the effort is focused towards innovation rather than identifying real/existing needs. For example, in the US important effort is invested in financial investments in testbeds and demonstration projects before identifying a market to deliver the innovations. This represents a particular understanding of the historical process in which, many times, markets followed innovation in the USA. In contrast, Germany has a clearer national strategy to integrate IoT into its manufacturing processes. The project advanced the efforts to integrate the IIoT concepts into Industry 4.0 and proposed an architectural model that offers a better understanding of production economics in Industry 4.0 (Radanliev et al., forthcoming-a).

- **Improving Quality of Service (QoS)** can be achieved by improving the predictive analytics in IoT mobility systems. The value is for both the operator (new revenue streams) and for users (improved QoS experience). For example, the Smart Road and Street Maintenance, Pricing and Planning (RoadMaPP) project identified ways in which users’ trust can increase in an econometric frame (Latinopoulos et al., 2018). The project developed a methodological framework to quantify the user impact of prediction reliability in IoT-enabled mobility services. It then applied the framework to London’s bike-sharing scheme.

The results demonstrated the impact of predictive algorithms on the QoS of transport services and highlight the value of data collection for empirical estimations. The results can improve the business proposition for service operators that have, for example, limited resources and uncertain demand and a lot of real-time information.

- **Combining all the aspects mentioned above** in order to optimise revenue has important applications also in the energy sector. For example, the P2P-IoET project worked with companies that were participating in initial coin offerings (ICOs) in order to understand the economic structures that allow investors to gain both personal and community-scale awareness. A possible application of this work is represented by the creation of new business models that can allow people to install IoT devices in buildings.

**RF3: Risk and Trust**

Risk and trust can be seen as different sides of the same coin and have major social implications. These aspects were explored in different ways in PETRAS research hub.

- The IAM project proposed an efficient way to quantify IoT risk – filling a major gap. One challenging aspect is that IoT risk is not included in cyber security assessment standards. Therefore, IoT risk is often not visible to cyber security experts. Companies integrating IoT devices and services need to perform a self-assessment. This defines a current and target state, prior to creating a transformation roadmap outlining tasks to achieve the stated target state. A comparative empirical analysis of multiple cyber risk assessment approaches could define a high-level potential target state for a company integrating IoT devices and/or services. Proposed design principles include a new transformation roadmap that adapts IoT risk impact assessment with a goal-oriented approach and the IoT Micro Mort model. An illustration of these principles is shown in Figure 4.2.
The Blockchain Technology for IoT in Intelligent Transportation Systems (B-IoT) project explored together with people from XAIN AG a way to significantly reduce the high energy consumption for mining in blockchain applications, with practical adaptation of existing technology used in the automotive sector (Lundbaek et al., 2018a, 2018b). This technique opens up the possibility of multiple commercial applications. For example, future vehicles can be turned into service platforms where different businesses, from energy suppliers to delivery and banking services, can trade and deliver automatic services. The project also explores how the notion of trustworthiness is changing as IoT-based systems become able to capture critical social aspects in the mobility sector. For example, access control over machine permissions can be assured in real-time and securely.

- The Designing Dynamic Insurance Policies using IoT (DDIP-IoT) project explores mechanisms that allow consumers to trust dynamic insurance services and protect different participants in the related shared ecosystems (see Box 4.3). The project develops mechanisms and formal models to manage dynamic insurance policies using IoT. It also provides a framework to create policy for cyber insurance that integrates real-time IoT-generated data to the current models used in the cyber insurance sector. These steps allow innovative ways to understand and design cyber insurance services to use IoT data: (a) to mitigate risk management and facilitate new developments in this area, such as risk engineering; (b) to increase transparency and predictability of the assurance and insurance aspects and processes, including near real-time evidence-based explanations meant to increase trust and reduce risks; (c) to increase the flexibility and adaptability of the current business environments, including through correlation of multi-model information such as risk, anomaly scores and liability; (d) to investigate the use of smart contracts to manage cyber risks within the insured environment.

- The National and International Policy for Critical Infrastructure Cybersecurity (NIPC) project focuses on one article on cooperation between actors to achieve IoT governance. This can be further extended by exploring the relation between minimisation of risk and increase of trust in ports and in the maritime industry in terms of international cooperation and trade (see Box 4.4). The project formulates policy recommendations for the cyber protection of UK critical infrastructure in an international context.
Despite the many challenges in understanding the types and nature of cyber risk and their dependencies/interactions in the IoT space, there are acceptable ways to assess the economic impact of IoT and its risks. One method is to use mathematical formalisms. Since the available historical data are non-existent for new technologies, the focus should be on a risk assessment approach that aims to evaluate the future, rather than explain the past.

The multiple complexities in calculating the economic impact of IoT cyber risk lead to the conclusion that impact can only be assessed with new risk metrics, combined with a new regulatory framework and standardisation of IoT risk databases. New risk vectors need to be identified and defined in the form of International IoT Asset Classification and Key IoT Cyber Risk Factors. This research Stream identified and presented some (but not conclusive) sets of new risk metrics, which emerge from adapting established methods for calculating risks and uncertainties.

The research Stream proposes a classification of cyber risk assessment requirements (identification, estimation and prioritisation) and combines common basic terminology, common approaches and incorporates existing standards, recommending a new model for calculating the economic impact of IoT cyber risk. The new risk metrics are to measure the IoT risk, while the risk model is to establish an acceptable IoT risk level. The model determines the maximum loss sensitivity and enables adjusting the acceptable IoT risk level, by calculating the risk metrics from new operating conditions. It also integrates established risk assessment approaches with existing cyber risk assessment frameworks to develop a tool for calculating the economic impact of IoT cyber risk (see Figure 4.3).
The new epistemological framework for impact assessment of IoT cyber risk (apply constructivist grounded theory methodology, drawing on knowledge from existing cyber risk frameworks, models and methodologies)

1. Consider finding from the 14.0 trends
2. Recommendations from the leading cyber risk frameworks
3. Quantitative model is needed that would be applicable to IoT cyber risks
4. ISO 27031 provides recommendations for disaster recovery. The other frameworks and the cyber risk models should integrate the conclusions from the ISO framework
5. The proposed design principles suggest anticipating recovery planning in the assessment of economic impact of IoT cyber risk
RF4: Value Creation in New Technologies and Standards

These aspects refer to the potential value creation in new IoT technologies and the standardisation effort that would support the marketability and adoptability of IoT products and services. The challenges include the need to move to new business models that are based around different regulations.

A pilot research effort with Porsche shows that a blockchain solution embedded in cars enables tracking and data hashing safely while users are in control of their data.

- The B-IoT project performed conceptual work on the practical use of blockchain technology in the mobility sector and tested this work in a pilot with Porsche in the first blockchain solution embedded in cars. The new technology allows tracking and safely hashing data while users are in control of the data. The modern vehicle generates 25GB data per hour, so one major challenge is how IoT-based systems can control and access this volume of data securely. As a result of this work, Porsche now is considering integrating blockchain in production by 2022, which represents a fast time to market in the industry. This move generated important changes in the entire industry and beyond, e.g. the creation of Mobile Open Blockchain Initiative (MOBI) that aims to create a service ecosystem in the automotive sector based on blockchain infrastructure. This is exemplary for the dynamics in IoT value creation in a highly competitive sector with relatively small margin supply chains.

- The adoption of new technology and standards in the international IoT governance and cooperation sector is essential. One major direction for further development of the NIPC project, for example, is represented by the way in which the global IoT infrastructure would contribute to a low-carbon economy.

- The P2P-IoET project explores the regulatory and social consequences when moving towards new technology, standards and business models based around outcome-based policy metrics and different regulation models. For example, it questions how regulators can incentivise and authenticate the process of energy reduction.

- The BlockIT project proposed an infrastructure to support reliable and cost-effective transactive energy, based on blockchain and smart contracts (Lombardi et al., 2018). Functionalities of this infrastructure, such as energy exchanges, storage of energy transactions and mitigation of cyber-attacks that exploit known vulnerabilities of smart meters, are implemented as fully decentralised applications and stored in the blockchain. Energy auctions can be carried out according to transparent rules implemented as smart contracts, hence visible to all involved actors.
IOT, GOVERNANCE AND CRITICAL INFRASTRUCTURE: THE INTERNATIONAL MARITIME SECTOR

The NIPC project examines policies to regulate critical national and international infrastructure that is increasingly incorporating IoT. The project will deliver an article on governance approaches, looking at cooperation to improve cybersecurity. The maritime sector is one critical form of infrastructure that is covered in the research.

In the maritime sector, IoT is largely focused on shipping rather than port facilities. A recent report shows that two-thirds of the shipping sector is interested in the potential of IoT but very few companies are doing anything in this field (Immersat, 2018). The exception is represented by big players, such as Maersk, who feel they should protect their business and also have the resources and scale to invest in IoT. This can represent a challenge in terms of diversity of operators on the market that can afford the important initial investment and continuous management of critical IoT infrastructure.

IoT is likely to have a significant impact on ports and their role in managing the movement of a large diversity of goods and people. Worldwide, over 80% of all goods move through ports, in the UK 85–95% of all imports come through ports. The efficient and timely movement of both goods and people is necessary as any disruption costs vast amounts of money. There is a shared belief in the sector that IoT and AI can improve logistic efficiency and supply chains in general, especially where the margins for profits are so narrow.

Many of the carriers and operators working in ports feel threatened, on the one hand, by the potential advantages brought by IoT to their competitors, and on the other hand by new big players moving into the sector. For example, according to one shipping industry expert, Google and Amazon are investing in automated shipping and are actively looking at the prospect of becoming important players in the movement of goods around the planet. Such a move would threaten the current business models in ports. It will have implications for adjacent sectors, such as insurance and transport.

An important aspect in terms of new business models enabled by IoT and AI is the relationship between the emerging political economy and issues around climate change and sustainable consumption. For example, distribution of goods would use IoT primarily to optimise overall energy efficiency, including transport, routing, handling or storage decisions, especially in new environments such as future floating ports or large dry ports. There is though limited attention in current research to the interlinkages between innovations within sectors and the impacts climate change could have on proposed new business models. How will climate change, in connection with extreme weather events like hurricanes, impact the business case of IoT systems in the maritime sector?
CONCLUSION

The HEV Stream combined existing literature and performed comparative, empirical and theoretical analysis in order to consider developments around harnessing economic value in IoT. The Stream mapped the existing initiatives for assessing the impact of cyber risk. This advanced the efforts of integrating cyber risk standards and governance. As a future research agenda, we need to better understand the holistic assessment for IoT cyber risk. This could be achieved by mapping the interactions among different factors in IoT devices and, in the process, deriving new sets of cyber security assessment and design criteria specific to cyber risk from the IoT. This would enable the visualisation of IoT cyber risk and inform best practice.

In addition, a transformational roadmap needs to assess the economic impact of IoT trade-offs between different aspects discussed in this chapter. These trade-offs should be considered at different levels in IoT systems, from IoT devices to IoT systems of systems and from engineering to organisational, managerial and strategic levels. The roadmap is also needed to visualise and assess exposure to cyber risk and to design implementation tasks for cyber recovery. This future research agenda would address critical sectors, such as critical infrastructure and I4.0 networks and national and international initiatives.

The lack of recovery planning confirms that many national initiatives are still unprepared for I4.0 and its associated cyber risks. The proposed future area of research would then enhance the visualisation and decomposition process of the required cyber capabilities and cyber recovery planning that are, surprisingly, not covered in the existing models. These processes would enable central governments to build national strategies that can respond to technological changes. The proposed decomposition of operational systems would enable workable action plans.

Finally, we need to further investigate the long-term economic value that depends on the data becoming a traded and reused commodity in real time and at high frequency, due to M2M automation for example, with citizen engagement at scale. This task requires a constant attention to emerging business models that consider the value and utility of IoT data and how these change over time. We need to understand better how to gain effectiveness and optimisation in complex IoT systems with the clear aim of improving well-being and the general quality of life. More research into the social consequences of IoT is needed and potential negative aspects should be tempered by national and international policies and agreements. This includes important and constant investment in education to secure the required digital skills and social understanding of emerging risks related to IoT and their mitigation.
REFERENCES


Approaches to dynamically visualise privacy, security and automation risks need to be advanced to make discussions on IoT accessible and inclusive.

There is a need for longitudinal studies – using both quantitative and qualitative, case study-based methods – of user attitudes, adoption, use, trust in, knowledge and experience of the IoT.

User-provider relationships must be clarified and made transparent, using everyday language wherever possible.

Empowering users with transparency and choice will support sustainable economic models based on the IoT.

The use of speculative methods to inform policy can help predict and accommodate potential social problems emerging from IoT adoption.
STANDARDS, GOVERNANCE AND POLICY
SAFETY AND SECURITY
PRIVACY AND TRUST
HARNESSING ECONOMIC VALUE
ADOPTION AND ACCEPTABILITY

House Training the Internet of Things (HTIoT)
Child Proofing the Internet of Things (IoT4Kids)
Developing a Consumer Security Index for Domestic IoT devices Plus (CSI+)
User-centric Adoption of IoT (UDAIoT)
Smart Transactions in Public Spaces (STiPS)
Displays on Smart Campuses (DiSSC)
IoT in the Park
Respectful Things in Private Spaces (ReTiPS)
INTRODUCTION

The objective of the Adoption and Acceptability (A&A) Stream is to contextualise the fundamental IoT research conducted by PETRAS and its partner organisations in terms of the factors that shape the adoption and acceptability of IoT products and services, now and in the near future. By understanding how users’ experience and perceptions of the IoT interact with adoption patterns, the Stream aimed to provide an accessible means for IoT product and service providers and users to leverage the benefits of IoT, whilst balancing the risks. Through a multidisciplinary approach, we researched and communicated ways to encourage development of useful and usable IoT technologies and devices. The Stream plays an integral part in the overarching aim of PETRAS to position the UK as a global leader in the design, manufacture and deployment of IoT products and services.

Given the rapid evolution of the IoT ecosystem, the challenge of understanding adoption and acceptability is not straightforward. Many interlinked factors may combine to impact on the acceptability of an IoT device or service, and how it is adopted and used. A central problem for acceptability is trust and how this is shaped by the user’s everyday experiences of a technology (Clarke et al., 2006). Various issues are relevant here in relation to the IoT: the ever expanding variety of IoT products and services; interacting with, making sense of and controlling complex, interconnected, self-adapting systems; design affordances for user-driven (re)configurability; data privacy and security; reliability in performance; and (un)predictability of behaviour. These are some of the key themes with which the Stream has engaged.

In our initial gap analysis (Skatova et al., 2017) covering relevant research on adoption and acceptability, we identified a number of specific non-technical issues with the IoT which were not covered by other IoT A&A projects and where further research was needed. All the issues that were identified in our gap analysis have been addressed in our Stream, and new ones emerged, pertaining in particular to theories and methods for researching the IoT.

Our findings reveal that new and bespoke approaches are needed that unpack and respond to the nuances of adoption and acceptability in a variety of IoT contexts. In partnerships with a range of PETRAS partners, including the consumer rights organisation Which? and the BBC, the Stream has explored how to address the complexity of IoT adoption by using a range of research approaches.

- Clarification and development of theories of adoption, acceptability and acceptance – how do these notions overlap and diverge in the scientific literature?
- Identification, exploration and interrogation of up-to-date models of technology acceptance – how might these models be applied to the IoT?
- Design, delivery and analysis of a nationally representative consumer attitudes survey – do user opinions cohere with acceptance models?
- Construction, experimentation and communication of near futures – how will IoT technologies and devices become domesticated and affect our lived experience?

This spectrum of approaches, supported by a range of workshop activities, has enabled the Stream to provide cross-cutting insights that will help drive responsible IoT innovation with the PETRAS projects. To achieve this, we collaborated with a range of PETRAS projects including: House Training the Internet of Things (HTIoT), Child Proofing the Internet of Things (IoT4Kids), Developing a Consumer Security Index for Domestic IoT devices Plus (CSI+),
User-centric Adoption of IoT (UDAIoT), Smart Transactions in Public Spaces (STiPS) and Displays on Smart Campuses (DiSSC). Capitalising on a strong alignment with the other PETRAS streams, the Adoption and Acceptability Stream provides a crucial set of use- and user-focused perspectives on the overall IoT landscape.

INSIGHTS

Bespoke Research Approaches for Engaging with IoT Adoption

Our gap analysis and literature review identified several areas of IoT research relating to adoption and acceptability as key areas for the future. With a focus on how the IoT is changing and the factors by which this is shaped, we identified a lack of longitudinal studies of user adoption, knowledge and experiences of, and trust, in the IoT. Further, there is a need to track at scale through opinion and topic mining how attitudes to IoT evolve and are influenced by events (such as data breaches, criminal actions, etc.) as these propagate through and are debated in online platforms such as Twitter and Reddit (Zubiaga et al., under review). Our examination of methods and approaches for unpacking technology adoption demonstrate that the unique challenges posed by the IoT demand new methods able to respond to the heterogeneity of IoT alongside the rapidly changing landscape. Through the Stream’s research we have developed several frameworks and metaphors to deal with these gaps, including the benefit attribute (Cannizzaro and Procter, forthcoming), ‘acceptable’ adoption studies (Cannizzaro et al., forthcoming-a), an IoT-adapted version of the Unified Theory of Acceptance and Use of Technology (UTAUT) (Cannizzaro et al., forthcoming-b), the IoT constellation metaphor (Lindley et al., 2017b) and the role of speculative methods in developing Implications for Adoption (Lindley et al., 2017a).

Figure 5.1 Constellation diagram
Strategies for Clear and Transparent Communication

By networking and collaborating with PETRAS projects we further developed a range of insights. These include the need to make discussions relating to the IoT more understandable by developing ways of visualising privacy, security and automation risks more dynamically. There is a need for clear explanations of meaningful benefits of IoT to users. User/provider relationships must be clarified and made transparent wherever possible. Everyday language can support these endeavours. Public behaviour-change campaigns may support healthy engagement with the IoT, while utilising speculative methods to inform policy may help to predict and accommodate potential social problems emerging from IoT adoption. The development of industry or government backed labelling schemes to communicate IoT-relevant factors to consumers and articulate how new business models impact consumers will help to improve acceptance.

Proactive and Adaptable Governance

Further funding to explore how to regulate and, where necessary, police IoT products and services will be necessary to keep pace with adoption. Promoting and facilitating the delivery of value-driven products that empower users by offering transparency and choice will assist sustainable economic models based on the IoT. Leveraging the UK’s influential position with respect to evolving global data governance legislation presents an opportunity to be proactive rather than reactive. Meaningful education at all levels, from early years to university to professional development, is essential to help maximise economic and social outcomes stemming from the IoT.

Figure 5.2  Concept label created as a provocation to explore how tropes from food labelling may be applied to consumer IoT products

Figure 5.3  Adapted Public Service Announcement poster used in support of the ‘Informed by Design’ research paper presented at the inaugural PETRAS conference. The paper explores how hubristic approaches to ‘Privacy by Design’ may actually lead towards privacy concerns.
RF1: UNPACKING ADOPTION AND ACCEPTABILITY

Adoption and acceptability are two of the perspectives typically associated with studies of how technological innovations diffuse through and are taken up within society. Simply put, a technology is acceptable to its users if it is instrumentally beneficial. However, acceptability is also prescriptive, as it defines the way in which the technology ought to be desirable. In this sense, it is essentially a moral judgement (van de Poel, 2016). Acceptability refers to what is good and ethically acceptable about the technology. Adoption, on the other hand, is defined not as a qualitative judgement, but as a process – ‘starting with the user becoming aware of the technology, and ending with the user embracing the technology and making full use of it’ (Renaud and Biljon, 2008).

However, when adoption as a perspective is invoked in empirical studies, it is acceptance that is then referred to for its theoretical grounding. This is because technology acceptance models (TAM) are widely used in Science and Technology Studies (Venkatesh et al., 2003). In this context, acceptance is not a qualitative attitude expressed as a set of judgements as per de Poel’s notion of acceptability. Instead, it refers to the degree of acceptance of a technology, expressed numerically as correlations of independent variables influencing adoption, the dependent variable. Studies of IoT adoption have typically utilised variations of technology acceptance models: e.g. User Acceptance (Rothensee, 2008), the unified perspective on the factors influencing consumer acceptance of IoT (Gao and Bai, 2014), the value-based adoption model (Kim et al., 2017) and factors affecting the adoption of IoT services (Hsu and Lin, 2018). For this reason, these studies inevitably refer to acceptance as their theoretical grounding, effectively conflating adoption with acceptance.

In addition, acceptability and acceptance are also sometimes used interchangeably in the context of IoT studies (Moody and Woodcock, 2012). This is due to their link to ‘attitude’. In the Royal Academy of Engineering report on the IoT, it is noted that ‘Policymakers need to investigate the attitudes of the public if acceptability of the IoT is to be understood’ (Taylor et al., 2018: 36, emphasis added). In so doing, they link acceptability to the attitudes of companies or the public, whilst not engaging with a more substantial critical treatment.

Lastly, it is important to underline that studies investigating the adoption of the IoT are often exclusively framed by economic arguments. In three key studies published in the past two years, it is noted that the reason for looking into adoption is that ‘IoT is considered important for promoting economic development and technological innovation’ (Hsu and Yeh, 2017). Researchers also remind us of the potentially huge market value of the IoT, which may be worth between $3.9 and $11.1 trillion by 2025 (Hsu and Lin, 2018), a key reason to try to determine which factors drive IoT adoption. According to the authors, the examination of smart home service adoption, using the value-based adoption model, was aimed at achieving IoT commercialisation (Kim et al., 2017). With such a fixation on economics in the context of IoT studies, adoption aligns with (benefits) IoT producers and service providers rather than with potential users. Adoption thus brings questionable values (or ‘benefit attributes’) to the studies it frames, making them easy targets for criticism from the point of view of user, consumer or environmentalist groups, on the basis that they ignore wider societal interests.

The economic fixation of adoption, in the context of IoT, brings questionable values to the studies it frames, often criticised for side-lining wider societal interests.
5.1

THE LITTLE BOOK OF PHILOSOPHY FOR THE INTERNET OF THINGS

Building on theory and philosophy to understand the issues that the IoT presents us with has been a useful tool throughout PETRAS. In The Little Book of Philosophy for the Internet of Things, researchers representing several PETRAS projects describe how the theory has helped inform their thinking. This includes a range of approaches, such as: Object Oriented Ontology, to ask what it really means to be a thing; Hyperobjects, to understand the wider impact of individual objects; Heterotopias, to explore the meaning of different physical and digital spaces; how everyday concepts like Respect and Fairness are changed by the IoT; how the IoT impacts on Ownership; and how Accelerationism can help us to comprehend the pervasive impacts of IoT adoption (see Figure 5.4).

Figure 5.4 Mapping Foucauldian Heterotopias for the Internet of Things
RF2: UNDERSTANDING ATTITUDES

In order to refocus IoT adoption and acceptability studies onto the user, we devised a survey investigating consumer attitudes to the IoT. To frame our survey design, we carried out a systematic review of the first 50 results of the top ten Information Systems (IS) and Management Journals in 2018 (according to Scimago Journal and Country Rank). This review revealed that the main body of empirical studies on IoT adoption, acceptability and acceptance examined have been carried out in East Asian countries (e.g. Hsu and Lin 2018; Hsu and Yeh 2017; Kim et al. 2017; Hong 2016; Gao and Bai 2013). This regional bias suggests that Eastern Asia businesses and organisations may be more competitively placed than European ones to harness IoT for economic, societal and environmental betterment. In addition, there is a lack of IoT adoption and acceptability studies with a nationally representative sample, as the largest study consisted of 426 respondents (Karahoca et al., 2018). To fill these gaps, our survey is based on a nationally representative sample (built around age, gender and education level) of 2000+ respondents based in the UK.

There is also a theoretical-methodological gap in empirical, quantitative IoT research, as the aforementioned studies have leaned on modified versions of popular technology acceptance models, rather than testing more recent and comprehensive models such as the Unified Theory of Acceptance and Use of Technology 2 (Venkatesh, 2012). This synthesises constructs of previously published work in competing TAM (performance and effort expectancy, social influence, facilitating conditions, hedonic motivation, price value, habit, behavioural intention, use) and has been adapted to a consumer market such as that of the IoT for the home. The survey questions were based on these constructs, which we integrated with those of trust (Venkatesh et al., 2011) in specific IoT contexts, i.e. automation, privacy and security; play; and technology rejection as, to date, there are no IoT studies that incorporate rejection theories. Overall, the survey consisted of 43 closed-ended questions. The initial results reported here pertain to levels of adoption, trust, intention to use/continue using the IoT.9

---

9 Full results and analysis will be written up for publication.
Issue 1: Measuring Adoption

Awareness
There are significantly more people that have heard of the expression ‘smart home’ (90%) than of ‘Internet of Things’ (46%).

Ownership and usage of smart home devices currently on the UK market
Respondents own an average of 1.85 (s.d. +/- 2.39) smart home devices (including duplicate devices, e.g. two smart TVs). The most owned and used smart home device is the smart TV (40%), followed by the smart meter (28%) and the personal home assistant (18%); the most desired smart home device is the remote home control system (29%), followed by the smart meter (25%) and the personal home assistant (24%); the least desired smart home device is the WiFi bathroom scales (70%), followed by the smart oven (67%) and the smart washing machine (63%); the smart home devices that people are most undecided about are the smart door lock (19%) and the smart fridge (18%).

Experience of use
67% of respondents have experience of using smart home devices, the majority of which (39%) have been using them for two years or more. Only 10% of respondents use their smart home devices without taking advantage of their ‘smart’ features; the largest group use only some of the smart functionalities (35%); smart TV and smart meters are the devices whose smart features are more likely to be always used (23% and 22% respectively). 42% of respondents are unsure about how to use or understand the security settings of their devices. 45% of respondents are unsure about whether their smart home device exceeded their expectations. 58% of people agree that they will use or continue using their smart home devices, with 25% being undecided and 17% being against.

Figure 5.5 Current ownership and desire to own IoT devices
**Issue 2: Measuring Trust**

**Privacy and security**

Overall, 63% of respondents agree that the likelihood of a privacy data breach is high when using the IoT, with 47% believing that the impact of such data breaches will also be high. 53% of respondents agree that the likelihood of security breach-related incident is high when using the IoT, with 46% believing that the impact of such a breach will also be high.

**Automation**

Overall, 50% of respondents agree that they do not trust smart home devices to work reliably and this distrust increases with the age of respondent (p < 0.05).

**Data collection and use, including consent**

Overall, 59% of respondents agree that knowing that data about use are collected by IoT devices makes them less inclined to use them and this increases with the age of respondent (p<0.05).

Overall, more people (46%) do not trust companies not to use IoT data without their explicit consent than those (32%) who trust them to use it only with consent. Once again, distrust in how companies will use IoT data increases with the age of respondent (p<0.05).

Finally, 67% of respondents overall agree that knowing that their data can be gathered and used without their consent would put them off from owning/using an IoT device.

---

**Figure 5.6** I fully trust IoT devices to work reliably (1 = strongly agree; 5 = strongly disagree).

**Figure 5.7** Knowing that IoT devices allow companies to collect data about how I use them would make me less inclined to use them (1 = strongly agree; 5 = strongly disagree).

**Figure 5.8** I trust companies not to use data produced by IoT devices without my consent (1 = strongly agree; 5 = strongly disagree).
5.2

Developing a Consumer Security Index for Domestic IoT devices (CSI)

**SECURE BY DESIGN: A POLICY REVIEW**

In March 2018, in the *Code of Practice for Consumer IoT Security*, the Department for Digital, Culture, Media and Sport (DCMS) announced their intention to explore the role of an IoT security labelling scheme. In direct collaboration with DCMS and the Dawes Centre for Future Crime, the Consumer Security Index project examined how IoT security labelling schemes may inform consumer decision-making and incentivise manufacturers to ship products with greater security features. Their research assessed the acceptability of different labelling designs (seal of approval marks, graded labels and informational labels) with consumers and experts through literature reviews, experimental studies and workshops. This work was complemented by a systematic literature review of what crime can be facilitated by consumer IoT products. The outputs of the project have identified drivers and barriers to the uptake of labelling schemes and identified which labelling format may be most effective for IoT security. Outputs from this project were recently discussed in an invited interview with the American Psychological Association (https://www.youtube.com/watch?v=wbLrXqg_oO0&t=195s) and will be referenced in forthcoming Secure by Design publications from DCMS.

**RF3: ACCEPTABLE IOT FUTURES**

The ambition of PETRAS is to deliver an array of fundamental IoT research (e.g. sensors in smart campuses and communication protocols for autonomous automobiles), which spread across a variety of use contexts (e.g. domestic, infrastructure, commercial). The cross-cutting streams serve the purpose of contextualising the insights emerging from the fundamental research in terms of specific use contexts, through high-level research-focused lenses. How to represent a specific technology in a context of use, while appreciating one or more of the stream perspectives, is a challenge addressed by the Adoption and Acceptability Stream’s speculative methods and Design Fiction.

*The use of Design Fiction as a method of inquiry enables the articulation of broader issues, such as standardisation, risk and interoperability*
The Design Fiction method developed through the Stream involves the creation of several prototypes around a given technology theme (e.g. smart grids, domestic IoT devices). Working together as a whole, these prototype designs allow researchers to probe possible futures that incorporate the technological theme, and by doing so help us to understand the implications of that technology’s adoption (Lindley et al., 2017a). Utilising speculation in this way is a particularly useful strategy when considering a multiplicity of factors relevant to adoption and acceptability because it places newly prototyped IoT innovations in plausible situations where their impact on aspects of the other streams (e.g. privacy, ethics, trust) are made visible and can easily be interrogated. Building these speculations in collaboration with PETRAS projects has helped to articulate how broader issues such as standardisation, risk and interoperability may interact as drivers of adoption, and moreover, how they manifest as agenda items for designers, educators and regulators working in the IoT space.

We designed Polly, a product that we described as the world’s first truly smart kettle. The device is equipped with a whole host of IoT-enabled smart features, but it is the finer details of the speculative future within which Polly exists that help tease out insights relevant to the Stream. In Polly’s world, the product is accredited and certified by a (fictional) government regulator (‘OfIoT’). This body uses design criteria (e.g. complete transparency about what data the device uses, and where they go) and technical standards that must be adhered to (e.g. Minimum Necessary Datagram Protocol or MNDP) in order to gain accreditation. Prototypes reflecting these regulations include devices designed around simple-but-effective user interfaces that demonstrate how effectively regulated devices can disclose (rather than obfuscate) precisely what data the device uploads/downloads, and for what purpose. Helping to drive the impact of transparency-driven interface designs, implementing transmission protocols such as MNDP can provide a verifiable means for IoT manufacturers to demonstrate how their products behave as they claim (Lindley et al., 2017b).

Figure 5.9 Using Design Fiction to give foresight the gravitas of hindsight and explore plausible future implications for adoption
The European Union’s General Data Protection Regulation (GDPR) came into force during the PETRAS project (on 25 May 2018) and as such provided a crucial lens to consider IoT adoption and acceptability. With GDPR-compliant consent processes in mind we utilised Design Fiction to create another speculation, this time around an IoT-enabled door lock device. Once again, while the smart features are exemplars of how the IoT can impact on how we use everyday devices, more salient issues focused around personal data and privacy. Utilising the constellation metaphor we had previously developed, this project mapped all of the possible data relationships that may stem from one simple interaction with the IoT lock. Our aim was to explore how to navigate the challenges of gaining GDPR-compliant consent (i.e. verifiable, specific and unambiguous) in the context of the hyper-connected IoT. The project led us to create a prototype referred to as Privacy Orbits, a graphical display intended to help supersede traditional means of gaining consent which are largely text-based, cannot be changed over time and that offer no flexibility for users. This project informed an analysis and critique of how the GDPR utilises the phrase ‘Privacy by Design’, noting the potential for hubristic interpretations of the term and, instead, calling for more pragmatic attempts to design products that equip their users to become Informed by Design (Lindley et al., 2018).

The potential economic and social benefits of IoT technologies are vast. However, in order to enable those benefits the technologies must be adopted. This future-focused element to the Stream’s research explores and reflects on how adoption is inseparable from the foci of the other streams and from attributes contributing to trust such as heterogeneity, ownership, predictability and governance. In order to harness the economic and social benefits of the IoT, supporting governance structures must be defined in ways that balance requirements of all participants in any given IoT constellation (e.g. a user, service provider, manufacturer, government) and consider the core PETRAS themes, privacy of trust and security.
5.3

CREATIVE INTERVENTIONS

In order to better comprehend possible IoT futures, PETRAS has facilitated various design-led interventions. These include the introduction of internet connected gnomes in the Queen Elizabeth Olympic Park. The gnomes featured chatbots that could simultaneously provide historical information to park visitors, as well as being research probes to understand nefarious actors in IoT networks. The Bitbarista prototype utilised blockchain technology to allow coffee consumers to make price and/or ethically informed decisions when they purchased their coffee, helping to reveal how the IoT and blockchain can impact upon meaningful consumer choices (Pschetz et al., 2017) and the Ethnobot was designed and deployed to capture rich ethnographic data as participants move through outdoor space, using a chatbot metaphor (Tallyn et al., 2018b). A number of Design Fiction projects including Polly (a smart kettle), Orbit (a privacy-enhancing technology) and Allspark (a smart grid system) have helped visualise and challenge notions of how IoT adoption will impact upon broader acceptability of connected technologies.

Figure 5.12 The Bitbarista, blockchain enabled IoT coffee machine
CONCLUSIONS

The research undertaken as part of the Adoption and Acceptability Stream provides vital perspectives on how the outputs of PETRAS can keep pace with the fast-moving IoT landscape.

The Stream’s research has helped to develop theoretical models including the benefit attribute and IoT constellations for understanding the interplay between adoption, acceptability and the myriad of factors contributing to perceived levels of trust, such that researchers, businesses and policymakers are equipped to engage with how and why the IoT is impacting everyday life. A key takeaway of this Stream is the need to rebalance models in terms of a holistic nuanced view that includes, but does not solely focus on, the assumption that if IoT technologies are made available they will become desirable, acceptable and adopted.

This theoretical work that provides a richer contextualisation of what adoption and acceptability mean is supported by empirical elements:

- the energy-saving expectation behind smart home devices purchase;
- the uncertain expectation/satisfaction ratio;
- the low levels of trust in privacy and security;
- the fairly low level of literacy in smart device use;
- optimism to continue using the technology despite the above.

Unpacking adoption and acceptability, this evidence is cross-referenced further with other key PETRAS streams, including privacy, trust and security. Preliminary findings in this space extend and support the theoretical foundations, suggesting a fragmentation in user attitudes – while adoption of the IoT is broad and likely to continue, there is significant space to make the IoT more acceptable by reducing anxieties stemming from uncertainty relating to privacy, trust and security.

Finally, the Stream’s work argues for the importance of considering the broader implications of IoT adoption ahead of time. It has developed models and methods that IoT practitioners can utilise in order to achieve this sort of applied speculation. In our technologically mediated world, where disruptive innovation happens at breakneck speeds, there is a clear and present requirement to meaningfully consider not just what the IoT can do, but how and why it may come to pass. As the IoT becomes increasingly domesticated and connected, it is imperative that social and technical aspects of adoption and acceptability continue to be considered, such that we can maximise the benefits of the IoT, whilst anticipating and tempering the risks.
REFERENCES


Hsu, C and Yeh, C. 2017. Understanding the Factors Affecting the Adoption of the Internet of Things. Technology Analysis and Strategic Management, 29(9), 1089–1102.


CONCLUSION:
THE FUTURE OF IoT
CONCLUSION: THE FUTURE OF IoT

PETRAS’s endeavours to understand and tackle the challenges concerning the cybersecurity of the Internet of Things used multiple ‘lenses’ and resulted in key findings that will shape industrial responses, approaches from consumer groups, and the international and domestic governance of these emerging socio-technical systems. Through the lenses of the five Streams examined in this report, PETRAS’s research derives holistic recommendations, encompassing the technical, economic, human and social factors that shape the continuing development of IoT. Recommendations drawn from research across all these perspectives feed into five main actionable areas. These actionable areas address the main recommendations in the Blackett Review (2014), highlighting the need for continuous efforts to realise the full potential of IoT and promote its adoption.

FUTURE RESEARCH

In order to harness the considerable potential for the IoT to deliver economic and social benefits, facilitate the secure integration of interconnected systems, and improve the human condition, further physical and social science research is required to ensure the IoT can be safely and reliably implemented and adopted. In order for this to happen, it will be important to advance work on data trust models and the end-to-end assurance of IoT device and information provenance. It will also be critical to develop our understanding of risks as well as risk assessment methods across the broad spectrum of IoT application areas and domains. Further research is necessary to explore, with privacy assurance approaches, the distributional impact of new business models and consumer trust and experience of IoT, which will profoundly shape technology adoption. Ongoing development and refinement of different policy, regulatory, governance models and mechanisms are also essential.

STANDARDS, GOVERNANCE AND POLICY

Existing sector-specific policy, regulations and other governance mechanisms are increasingly recognised as unfit for purpose. They have slow response times and are difficult to integrate and to adapt to dynamic governance requirements as the IoT is adopted across society and diverse sectors, enabling new business models and the further convergence of technology, market sectors and industries. There is a consensus that policy, regulation and governance of IoT need to be adaptive, agile and flexible. Standards are expected to play a significant role as operational tools for implementing policy and regulatory principles across the diverse IoT application areas, domains and market sectors in which IoT has been integrated. Ongoing development and adaptation of approaches to implement and monitor compliance with existing as well as emerging standards and principles, particularly ones concerning security, privacy and transparency, are also necessary. Most importantly, effective governance of the IoT, enforcement of security as well as privacy principles, requires close international cooperation due to the fluidity of IoT product and service provision across various jurisdictions.

DESIGN AND DEPLOYMENT

The introduction of all new technologies influences human behaviours in both intended and unintended ways. Thus, there is always an inherent ethical responsibility on the part of the creators and deployers of new technologies to explore how these might affect existing behaviours and create new behaviours both pre and post deployment. Given the ever-evolving complex interdependencies within the IoT, coupled with sometimes contradicting value systems of stakeholders within these systems, the creators of IoT products and services are facing new challenges that will need new design and deployment approaches.
In particular, ethical considerations should be at the forefront of the design, functions, support, and maintenance of IoT products and services throughout their life cycle if IoT systems are to be adopted and accepted at scale. This should include security, privacy and transparency of operation in such a way that users are empowered within IoT deployments. Achieving this requires dynamic research, development and deployment that takes a holistic socio-technical view that can more fully address the complexities of the continually evolving network ecologies of IoT. In particular, there is a need for longitudinal studies of the situated deployments of IoT – using both qualitative and quantitative methods to understand user attitudes towards and experience of IoT. Whilst large scale quantitative studies can yield general understandings of interactions with IoT products and services, they need to be combined with qualitative studies that allow for complexities of context of use to be revealed which are often outside what can be derived from interaction derived data alone.

BESPOKE RESEARCH APPROACHES FOR ENGAGING WITH IOT ADOPTION

The gap analysis and literature review carried out by PETRAS researchers identified several areas of IoT research relating to adoption and acceptability as key areas for the future. This research identified a lack of longitudinal studies of user adoption, knowledge and experiences of, and trust in the IoT. Further, there is a need to track at scale through opinion and topic mining how attitudes to IoT evolve and are influenced by events (such as data breaches, criminal actions, etc.) as these propagate through and are debated in online platforms such as Twitter and Reddit. The unique challenges posed by the IoT demand new methods and approaches for unpacking technology adoption. Through research, PETRAS has developed several frameworks and metaphors to deal with these gaps, including the benefit attribute, ‘acceptable’ adoption studies, an IoT-adapted version of the Unified Theory of Acceptance and Use of Technology (UTAUT), the IoT constellation metaphor and the role of speculative methods in developing implications for Adoption.

EDUCATION

Multiple aspects of educational initiatives need to be considered in order to achieve the full potential of the IoT. First, consumers should be better supported to make choices that align with their expectations of data security and privacy as well as the safety issues that emerge from the implementation and adoption of the IoT. Without adequate market drivers for clearly informing consumers of the risks and of their rights with regard to IoT devices, services and systems, governments will have a role to play in designing initiatives that will meet this requirement. Secondly, education from primary to tertiary levels must adapt from purely discipline-specific to inter-disciplinary approaches that help students understand the interdependencies and interconnecting dynamics of technology, ethics, markets, law, governance etc. And finally, it is important that decision makers in both industry and policy communities are supported to incorporate these same interconnected dynamics through greater technical literacy so that the interplay between privacy, ethics, trust, reliability, acceptability and security are incorporated into their risk analysis and decision-making processes.

In order to fully capitalise on the significant potential of the IoT, it will be important to take a holistic, coherent approach to pursuing opportunities and managing the attendant cyber security challenges. This next phase of networked systems will draw lessons from the past 25 years of Internet technology but it will also push beyond them. The IoT will demand levels of coordination, transparency, accountability and collaboration that extend past practices in this domain. It will also bring to light value systems and expectations that may not always align but will need to be accommodated. If this is delivered in ways that benefit society and avoids alienating key stakeholders, the potential for economic growth and improving the human condition is considerable. The research generated by PETRAS over the past three years will be a key contribution to reaching these goals.
APPENDIX 1: PETRAS PROJECTS AND STREAM ALIGNMENT
APPENDIX 1: MAPPING OF THEMES AND AREAS OF EXPERTISE
APPENDIX 2:
LIST OF PETRAS PROJECTS
REFERENCED IN THIS REPORT
APPENDIX 2:
LIST OF PETRAS PROJECTS REFERENCED IN THIS REPORT

01 STANDARDS, GOVERNANCE AND POLICY
- Data Sharing in the IoT (PEDASI) Demonstrator
- IoT Multi-disciplinary Standards Platform (IoT-MSP)
- Developing a Consumer Security Index for Consumer IoT Devices (CSI)
- House Training of the Internet of Things (HTIoT)
- Cyber Risk Assessment for Coupled Systems (CRACS)
- National and International Policy for Critical Infrastructure Cybersecurity (NIPC)
- Designing Dynamic Insurance Policies using IoT (DDIP-IoT)
- The Internet of Every Things (P2P-IoET)
- Gender & IoT (G-IoT)

02 SAFETY AND SECURITY
- Cyber Risk Assessment for Coupled Systems (CRACS)
- Blockchain-empowered Infrastructure for IoT (BlockIT)
- The Internet of Every Things (P2P-IoET)
- Blockchain Technology for IoT in Intelligent Transportation Systems (B-IoT)
- Analytical Lenses for IoT Threats (ALIoTT)
- IoT in Control (IoTinControl)
- Newcastle Urban Sciences Building IoT (NUSBioT)
- Security Risk Assessment of IoT Environments with Attack Graph Models (SECRIS)
- Impact Assessment Model for the IoT (IAM)
- Designing Dynamic Insurance Policies using IoT (DDIP-IoT)
- Geographic Personal Data and Location Based Services (GeoSec)
- Security and New Threats in Healthcare (SeNTH)
- Security and New Threats in Healthcare+ (SeNTH+)
- Potential Impact of IoT Boosted Botnet Attacks (BotThings)
- Securing IoT in Critical National Infrastructure (SecCNIoT)

03 PRIVACY AND TRUST
- Blockchain Technology for IoT in Intelligent Transport Systems (B-IoT)
- Displays and Sensors on Smart Campuses (DiSSC)
- Data Analysis in IoT Solutions for Healthcare (DASH)
- Respectful Things in Private Spaces (ReTiPS)
- Displays and Sensors on Smart Campuses (DiSSC – Campus)

04 HARNESSING ECONOMIC VALUE
- The Internet of Energy Things (P2P-IoET)
- Economic Value of IoT Data in Cyberphysical Supply Chains (EVIoT)
- Value of Personal Data in IoT (VPD)
- Smart Transactions in Public Spaces (STiPS)
- Impact Assessment Model for the IoT (IAM)
- Smart Road and Street Maintenance, Pricing and Planning (RoadMaPP)
- Blockchain Technology for IoT in Intelligent Transportation Systems (B-IoT)
- Designing Dynamic Insurance Policies using IoT (DDIP-IoT)
- National and International Policy for Critical Infrastructure Cybersecurity (NIPC)
- Blockchain-empowered Infrastructure for IoT (BlockIT)

05 ADOPTION AND ACCEPTABILITY
- House Training the Internet of Things (HTIoT)
- Child Proofing the Internet of Things (IoT4Kids)
- Developing a Consumer Security Index for Domestic IoT Devices Plus (CSI+)
- User-centric Adoption of IoT (UDAIoT)
- Smart Transactions in Public Spaces (STiPS)
- Displays on Smart Campuses (DiSSC)
- IoT in the Park
- Respectful Things in Private Spaces (ReTiPS)