PETRAS

IMPACT REPORT

CONTENTS

A HISTORY OF PETRAS: HUB AND CENTRE

A Blackett Review on the 'Internet of things: making the most of the second digital revolution' was published in 2014.[1] Its recommendations identified socio-technical challenges concerning privacy, trust, security, etc. that needed to be addressed to release market opportunity for IoT, and that there was a requirement for research and technology demonstration across application sectors. DCMS was tasked with coordinating and funding these recommendations. It devolved its administration functions to IoTUK.

IoTUK was formed in 2015 and hosted within the Digital Catapult to accelerate the UK's IoT capability as part of the Government's £40 million investment in IoT. It played a central role in enabling IoT entrepreneurship, collaborating with organisations in a wide range of fields, including cities, health and industrial applications.[2] Two large-scale demonstrator activities were funded under IoTUK; CityVerve — a £10m Smart City programme in Manchester — and two Healthcare demonstrators (focusing on Dementia and Diabetes). Concurrent with the launch of IoTUK, EPSRC commenced administration of the research part of the DCMS remit, issuing a call (ComPaTrIoTS) in June 2015.

A university consortium led by UCL, with Imperial College London, University of Oxford, Warwick University and Lancaster University, began operating as a Hub with technical and behavioural science expertise. Four 'spoke' universities[3] and 20+ user partners collaborated to write the PETRAS proposal, including 17 project ideas, to bid into the ComPaTrIoTS Call. The consortium was successful, and a £9.8m award was made to the Hub in 2016. Pledges from 47 user partner supporters added £14m to this figure.

The PETRAS Hub operated between 2016 and 2019, executing 51 projects and six medium-scale (knowledge into practice) demonstrators. Ultimately, 11 university collaborators were involved, employing over 45 researchers collaborating with over 100 user partners from the public and private sectors. DCMS commissioned a consultancy to report on the value added by IoTUK initiatives, and the PETRAS Hub scored well.

When in 2018 UKRI was formed and began administering the Strategic Priorities Fund, the Research Councils were asked to nominate programmes having good prospects of impact. As a result, EPSRC prepared a bid to UKRI, 'Securing Digital Technologies at the Periphery of the internet' (SDTaP), to go beyond IoT and include emerging technologies at the Edge, with the intention of issuing a closed call to the PETRAS consortium. SDTaP was successful, and in 2019, £25m was awarded to EPSRC and Innovate UK to partner in an SDTaP socio-technical research initiative intended span a range of Technology Readiness Levels, from basic research (3–4) to deployment in applications (8–9). A PETRAS National Centre of Excellence bid was made and was successful, with a £13.8m award being made in 2019. Innovate UK received £11m to fund a sister programme of five demonstration projects led by industry. To promote optimum synergy and knowledge transfer, the PETRAS Centre and the Demonstrator programmes share common industry advisory and governance boards.

It has been my privilege and pleasure to direct PETRAS over seven years through its two phases, and to work with outstanding executive and academic teams. I have learned a lot, both about the subject of 'edge' cybersecurity and how cross-disciplinary approaches can contribute to understanding and solutions, and how a large multi-university team can work effectively together, and with user partners from public and private sectors.

Professor Jeremy Watson CBE FREng FIET
Director and Principal Investigator

The Quintet, led by Prof Jeremy Watson, provided expertise, insight and senior leadership advice to the PETRAS community and included:

Deputy Director of PETRAS, Prof Julie McCann FBCS and CEng, Imperial College London

Prof Tim Watson FBCS FIET, Loughborough University

Prof Rachel Cooper OBE, Lancaster University

Prof Dave De Roure FBCS FIMA FRSA, University of Oxford

[1] https://www.gov.uk/government/publications/internet-of-things-blackett-review
[2] https://www.gov.uk/government/publications/iotuk-the-worlds-leading-national-iot-programme
[3] Surrey (5G), Southampton (Web science), Edinburgh (Design) and Cardiff (International governance)

ABOUT PETRAS

PETRAS first received funding from EPSRC in 2016, and then from the UK Government's Strategic Priorities Fund between 2019 and 2023 to ensure that technological advances in Internet of Things (IoT) connected devices, including Artificial Intelligence (AI) and Machine Learing (ML), were developed and applied safely and securely.

PETRAS stands for: Privacy, Ethics, Trust, Reliability, Acceptability and Security and has:

- Taken into consideration both social and technical issues relating to cybersecurity of the IoT.
- Collaborated with industry and government partners to ensure that the research would be applied for the benefit of society, business and the economy.

WHY ARE IoT, AI and ML IMPORTANT?

PETRAS is interested in how interactions between these technologies produced cybersecurity challenges that need to be addressed if society and the economy are to harness their full potential benefit.

- Society increasingly relies on technologies such as the IoT and AI to enhance the quality, efficiency and sustainability of our lifestyles, goods and services; e.g., voice-controlled smart door locks for the home, to fully automated manufacturing and logistics systems.
- IoT, for both consumers and business, has seen a 600% increase in cybersecurity attacks since 2016. The impact of such attacks is more than technological – each successful attack can cause economic, social and environmental damage.

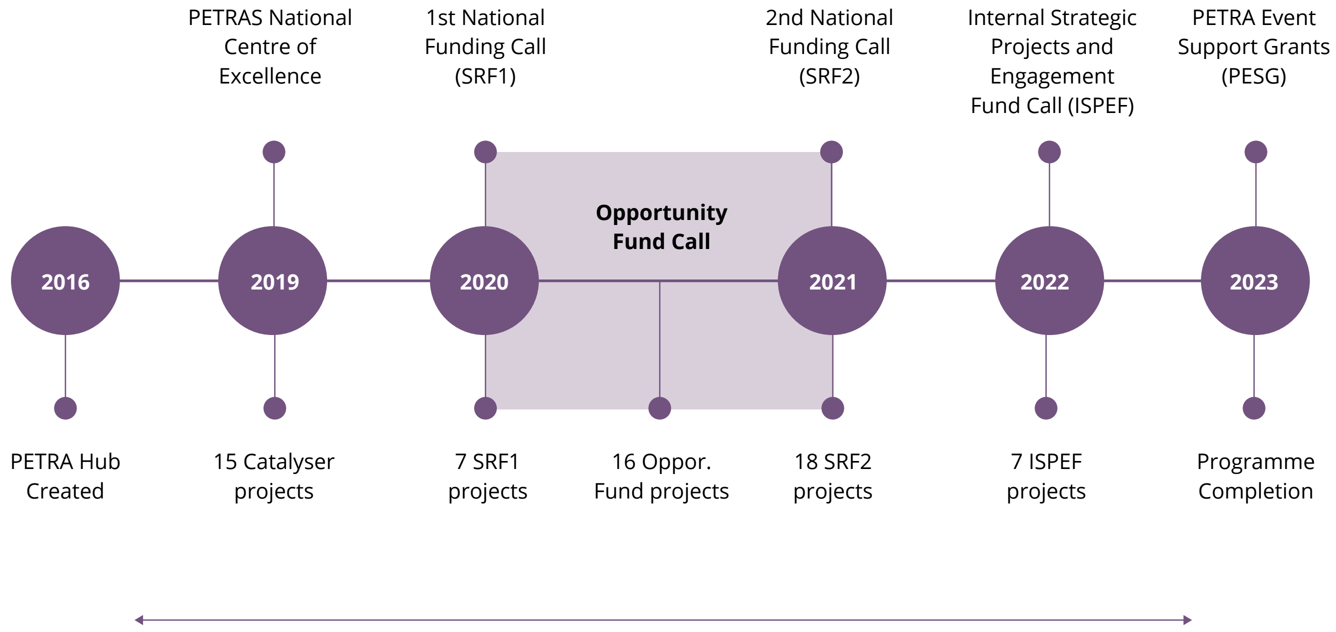
KEY CYBERSECURITY CHALLENGES ADDRESSED BY PETRAS

- Cybersecurity challenges include the security of; networks, applications, endpoints, identities, databases and infrastructure, the cloud, edge devices and mobiles. The intersection of social and physical aspects is evident in all these challenges, and a cross-disciplinary lens has been used to address them. PETRAS research included disaster/business recovery and continuity planning, end user education and the development of governance, regulations, policies and standards.
- From 2019, PETRAS received funding to undertake research with a particular focus on the cybersecurity challenges associated with edge devices including those that had AI or Machine Learning capabilities.

WHY IS A SOCIO-TECHNICAL APPROACH IMPORTANT?

Past experience shows that technical solutions often fail for social and behavioral reasons. Examples of this include lack of awareness, weak passwords, undeveloped cybersecurity 'culture' within organisations, and responsibility splits. By combining social and technical expertise in the co-creation of new systems approaches, tools and techniques, both social and technical hurdles are overcome simultaneously.

PETRAS TIMELINE


2016 – PETRA Hub Created

2019 – PETRAS National Centre of Excellence – 15 Catalyser projects

2020 – 1st National Funding Call (SRF1) – 7 SRF1 projects

Opportunity Fund Call – 16 Oppor. Fund projects

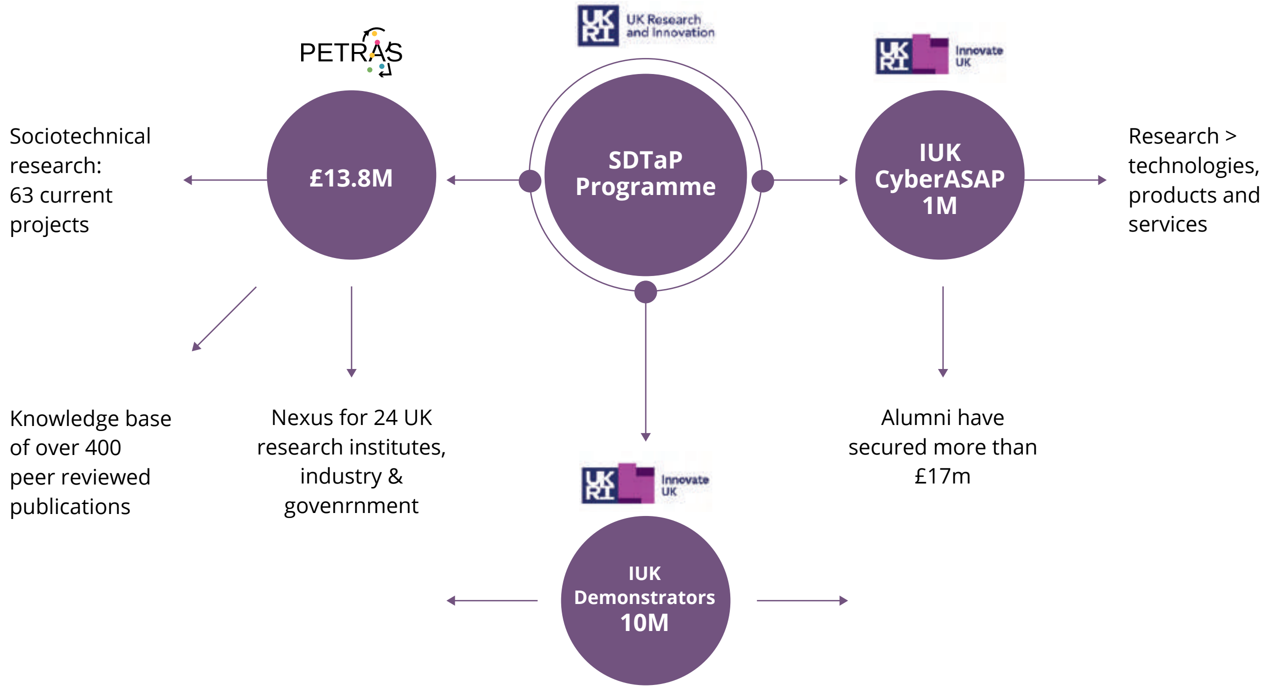
2021 – 2nd National Funding Call (SRF2) – 18 SRF2 projects

2022 – Internal Strategic Projects and Engagement Fund Call (ISPEF) – 7 ISPEF projects

2023 – PETRA Event Support Grants (PESG) – Programme Completion

UKRI'S ENSURING THE SECURITY OF DIGITAL TECHNOLOGIES AT THE PERIPHERY (SDTaP) PROGRAMME

The SDTaP Programme supports the development of a safe Internet of Things (IoT).


PETRAS £13.8M

SDTaP Programme

IUK CyberASAP 1M

IUK Demonstrators 10M

Sociotechnical research: 63 current projects

Research > technologies, products and services

Knowledge base of over 400 peer reviewed publications

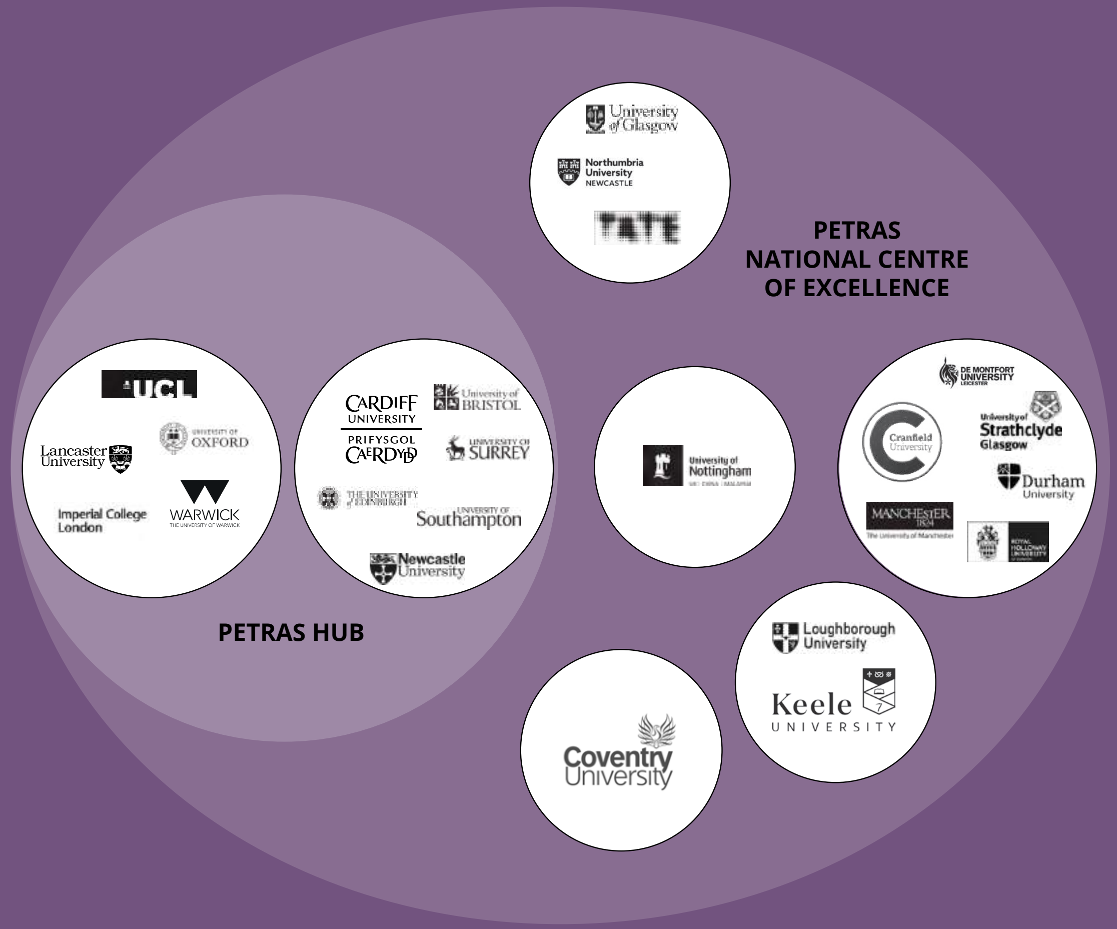
Nexus for 24 UK research institutes, industry & govenrnment

Alumni have secured more than £17m

ABOUT PETRAS

24 Research Institutions

University College London, Imperial College London, University of Oxford, Lancaster University, University of Warwick, University of Southampton, Newcastle University, University of Nottingham, University of Bristol, Cardiff University, University of Edinburgh, University of Surrey, Coventry University, Northumbria University, Tate, University of Glasgow, Cranfield University, De Montfort University, Durham University, University of Manchester, Royal Holloway, University of London, University of Strathclyde, Loughborough University and Keele University.


PETRAS NATIONAL CENTRE OF EXCELLENCE

PETRAS HUB

SECTORS RESEARCHED

- Agritech
- Ambient Environments
- Health and Wellbeing
- Infrastructure
- Supply Chains and Control Systems
- Transport and Mobility

RESEARCH STREAMS AND LENSES

PETRAS Hub (2016-2019)

- Harnessing Economic Value
- Privacy and Trust
- Safety and Security
- Governance and Policy

PETRAS National Centre of Excellence (2019-2023)

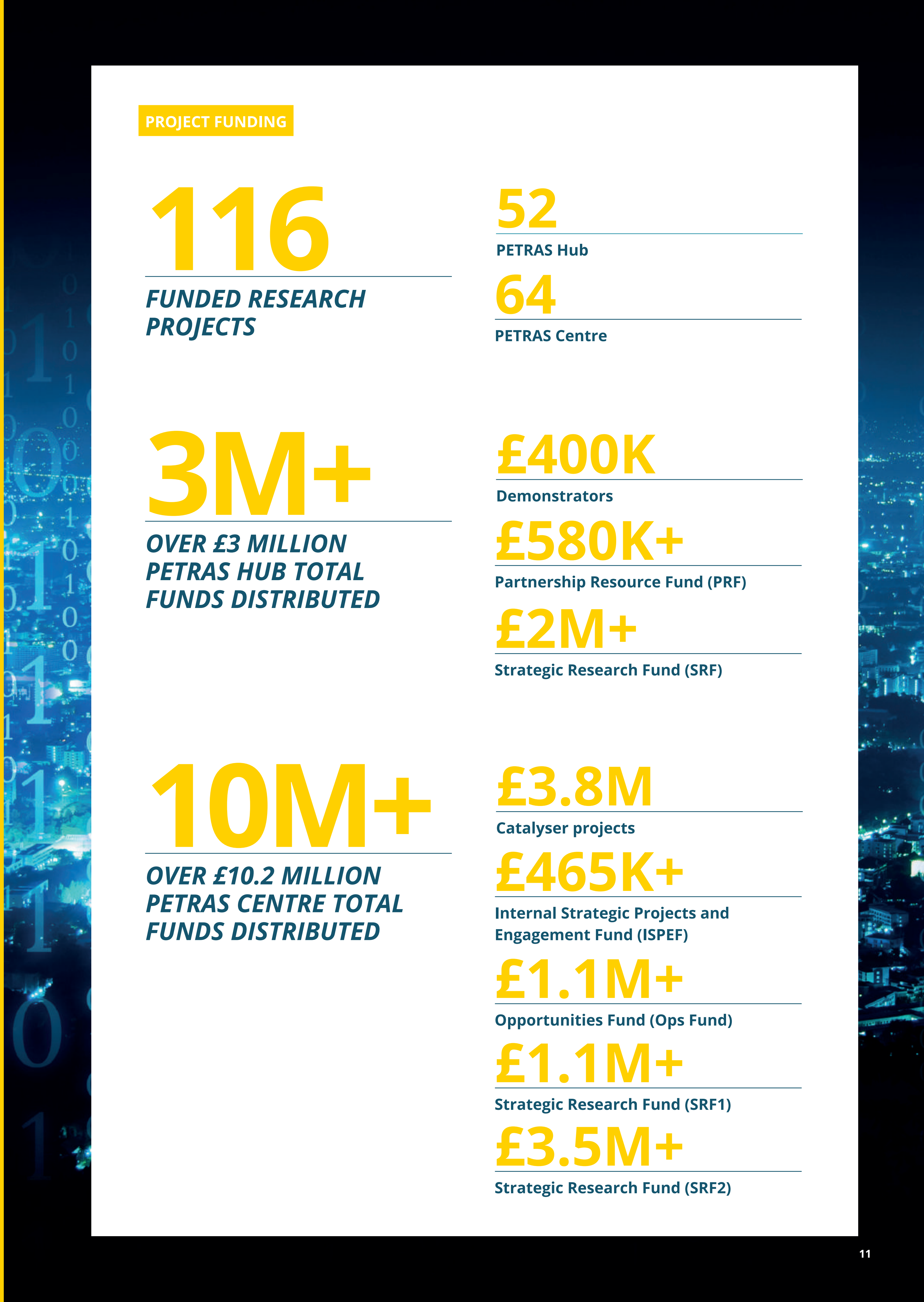
- Securing the Connected Edge
- Useful, Useable Decentralisation
- Law and Economics at the Edge
- Buidling Public Value at the Edge

PURPOSE OF THIS REPORT

To provide an overview of the entire evidence base funded by PETRAS would require a report many times the size of this one.

This report is a resource which can be used by those wishing to get an overview of notable PETRAS achievements in the areas of policy, research and industry.

We also point readers to the PETRAS Research Knowledge Base, where all the peer-reviewed and non-peer reviewed papers and analysis can be found (see p.32 for more information). Specific projects can be identified in the Appendix, depending on readers' interests.



PROJECT FUNDING

116

FUNDED RESEARCH PROJECTS

52	PETRAS Hub
64	PETRAS Centre

3M+

OVER £3 MILLION PETRAS HUB TOTAL FUNDS DISTRIBUTED

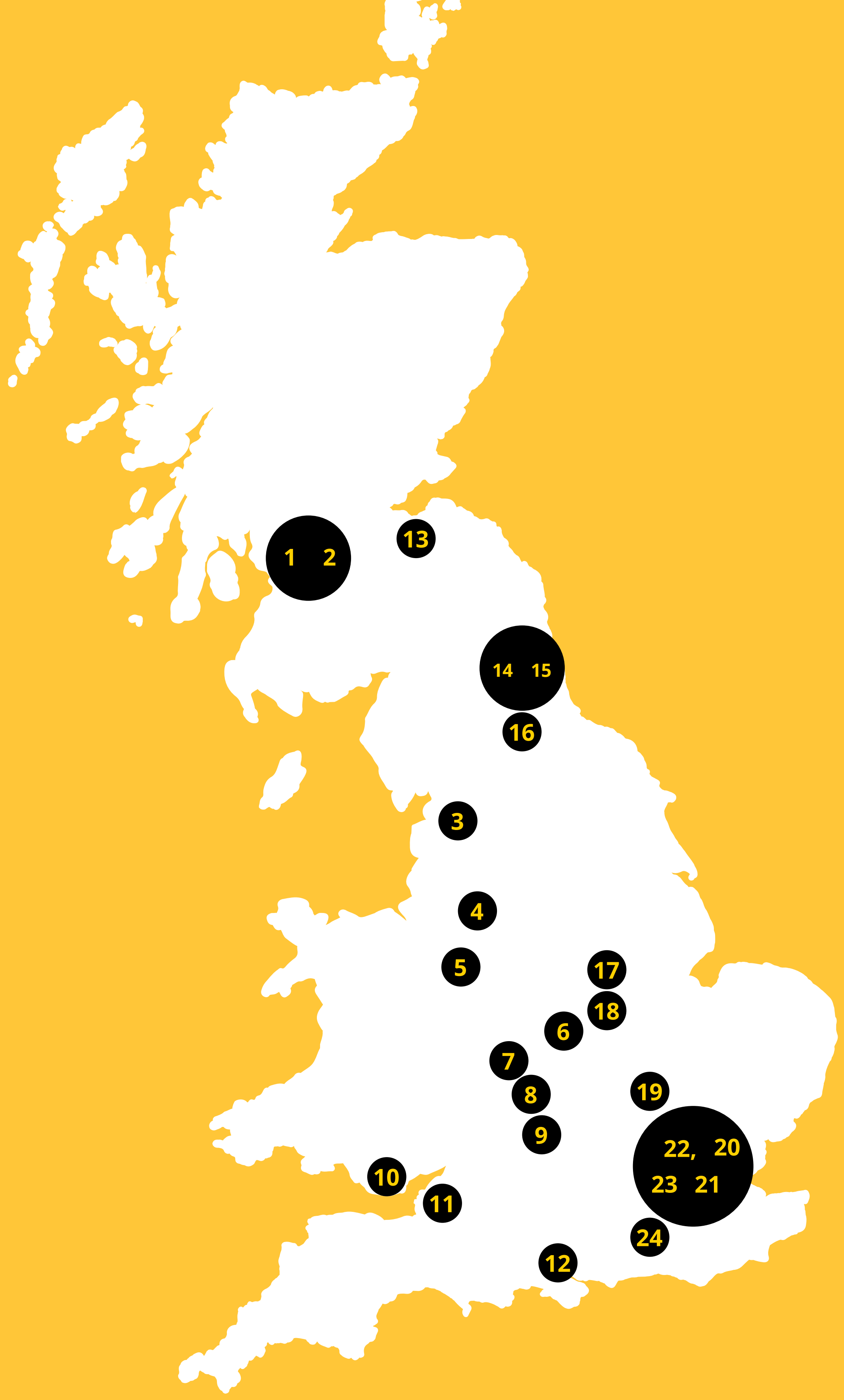
£400K	Demonstrators
£580K+	Partnership Resource Fund (PRF)
£2M+	Strategic Research Fund (SRF)

10M+

OVER £10.2 MILLION PETRAS CENTRE TOTAL FUNDS DISTRIBUTED

£3.8M	Catalyser projects
£465K+	Internal Strategic Projects and Engagement Fund (ISPEF)
£1.1M+	Opportunities Fund (Ops Fund)
£1.1M+	Strategic Research Fund (SRF1)
£3.5M+	Strategic Research Fund (SRF2)

PETRAS ACROSS THE UK



1. University of Glasgow
2. University of Strathclyde
3. Lancaster University
4. University of Manchester
5. Keele University
6. De Montfort University
7. Coventry University
8. University of Warwick
9. University of Oxford
10. Cardiff University
11. University of Bristol
12. University of Southampton
13. University of Edinburgh
14. Northumbria University
15. Newcastle University
16. Durham University
17. University of Nottingham
18. Loughborough University
19. Cranfield University
20. University College London
21. Tate
22. Imperial College London
23. Royal Holloway University of London
24. University of Surrey

PETRAS ACHIEVEMENTS

In 2019, PETRAS was awarded funding as part of the Strategic Priorities Fund (SPF), an £830 million investment in multi and interdisciplinary research across 34 themes.

SPF is funded through the government's National Productivity Investment Fund and managed by UK Research and Innovation.

The fund aimed to:

- increase high-quality multi and interdisciplinary research and innovation.
- ensure UKRI investment links up effectively with government research and innovation priorities.
- respond to strategic priorities and opportunities.

INFLUENCING GOVERNMENT POLICY

National policy making regarding emerging technologies, especially IoT and edge technology, is broad and complex, having cross departmental implications. Throughout both the Hub and Centre, PETRAS academics have been working with multiple programmes and officials to target critical issues.

For example, in 2018, the Department for Digital, Culture, Media & Sport (DCMS) commissioned the PETRAS Hub, to conduct two separate literature reviews. The first review focussed on industry recommendations for government to improve IoT security and the second was about current international developments around IoT security.

There were two aims to these reviews:

- identify the key themes emerging from the literature.
- and identify international consensus around core Security by Design principles for the IoT.

These reviews can be found on GOV.UK at https://www.gov.uk/government/publications/summary-literature-review-on-iot-security

More recently, PETRAS academics have been commissioned by the Department for Science, Innovation and Technology (DSIT) (previously DCMS), to undertake a literature review of how public perceptions of connected places can impact their sustainability and security.

Further policy impacts have been achieved through two 6- month secondments of a PETRAS Research Fellow into the Department for Transport, advising on the cybersecurity of rail systems.

The following case studies showcase how PETRAS projects engaged, influenced and co-created solutions with government, industry and academia to benefit society and the economy.

INFLUENCING LOCAL GOVERNMENT

It is recognised that local government are adopting or considering IoT and edge technologies to address a multitude of local challenges from NetZero to health care, and that resilience at this local level is a key part of national security. PETRAS research has been instrumental in highlighting the challenges of procuring, implementing and maintaining such technologies. PETRAS works closely with the Society for Innovation Technology and Modernisation (SOCITIM) and the Local Government Association (LGA) in building knowledge amongst the local government community.

UCL

PRODUCT SECURITY AND TELECOMMUNICATIONS INFRASTRUCTURE BILL DEBATE (UK)

PROJECTS

Geopolitics of IoT Standards (GISt) and Building Evidence Base for CoP Legislation (BECL)

TEAM

Prof Madeline Carr, Dr Saheli Datta Burton, Dr Leonie Tanczer, Prof Stephen Haile

PETRAS work was highlighted in parliamentary debates on an amendment to strengthen cybersecurity in children's products in the Product Security and Telecommunications Infrastructure Bill[1]

The Product Security and Telecommunications Infrastructure Bill is a regulatory scheme to make consumer-connectable products more secure against cyber-attacks.

In June 2022, during a reading of the Bill in the House of Lords (volume 823: debated on 21 June 2022)[2], the PETRAS UK Code of Practice for Consumer IoT Security: where we are and what next, was directly referenced by Lord Fox (Liberal Democrat) when presenting an amendment relating to child security.

The UK Code of Practice for Consumer IoT Security: where we are and what next[3] was co-authored by Saheli Datta Burton (UCL), Leonie Maria Tanczer (UCL), Srinidhi Vasudevan (UCL), Stephen Hailes (UCL), and Madeline Carr (UCL) and is downloadable on the PETRAS website: https://petras-iot.org/petraspublications/.

The report includes insights into how widely the UK Government's UK Code of Practice[4] has spread since its publication in March 2018. A report informed by PETRAS's Summary literature review of industry recommendations and international developments on IoT security[5], as part of the Government's Secure by Design[6] policy, aims to 'ensure consumer "smart" devices are more secure, with security built in from the start.'

[1] https://bills.parliament.uk/bills/3069

[2] https://hansard.parliament.uk/lords/2022-06-21/debates/00F84FA3-2582-4623-9CE2-3AE62E55F65A/ProductSecurityAndTelecommunicationsInfrastructureBill

[3] https://petras-iotorgpetraspublications/?tsr=The+UK+Code+of+Practice+for+Consumer+IoT+Cybersecurity%3A+where+we+are+and+what+next&tps_button=Search

[4] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf

[5] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf

[6] https://www.gov.uk/government/collections/secure-by-design

Newcastle University

CYBER RESILIENCE ACT (EU)

PROJECT

Robustness-as-Traceability: Secure and Legal Calibration Workflows in IoT (RoasT-IoT)

TEAM

Prof Shishir Nagaraja, Kaspar Ludwigsen

A paper on law and security by researchers from PETRAS Roast IoT project (Kaspar Ludwigsen and Prof Shishir Nagaraja: Newcastle University) has been cited in EU legislation via the new EU Cyber Resilience Act that seeks to ensure safer hardware and software[1].

The Commission's proposal for a new Cyber Resilience Act (CRA)[2] aims to safeguard consumers and businesses buying or using products or software with a digital component. The Act would see inadequate security features become a thing of the past with the introduction of mandatory cybersecurity requirements for manufacturers and retailers of such products, with this protection extending throughout the product lifecycle.

The problem addressed by the proposed regulation is two-fold. First is the inadequate level of cybersecurity inherent in many products, or inadequate security updates to such products and software. Second is the inability of consumers and businesses to currently determine which products are cybersecure, or to set them up in a way that ensures their cybersecurity is protected.

The proposed Cyber Resilience Act would guarantee: harmonised rules when bringing to market products or software with a digital component;

- a framework of cybersecurity requirements governing the planning, design, development and maintenance of such products, with obligations to be met at every stage of the value chain;
- an obligation to provide duty of care for the entire lifecycle of such products.

[1] https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739259/EPRS_BRI(2022)739259_EN.pdf

[2] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

INFORMATION COMMISSIONERS OFFICE (UK)

In early 2023, the ICO's Emerging Technology Team published their first Technology Horizons Report. The report examines the implications of some of the most significant technological developments for privacy in the next two to five years. This report includes a chapter on next generation IoT, that several members of the PETRAS Centre Team and community contributed to.

"The work and insight PETRAS provided to the ICO's foresight research into the intersection of emerging technologies with data protection and privacy has been enormously helpful. It has allowed us to build and develop our regulatory approaches towards critical technologies such as next generation IoT and the input provided will continue to support our work as we develop formal guidance for those seeking to use these technologies."

You can find the report and further information here: https://petras-iot.org/update/petras-contributes-to-icos-tech-horizons-report/

Tate Exchange - The Internet of Things
(Dan Weill Photography)

TAKING IoT FOR A WALK WORKHOPS

PROJECT

Participatory Policies for IoT (at the Edge) Ethics (P-PITEE)

TEAM

Dr Naomi Jacobs, Dr Lou Mullagh, Nuri Kwon

Local governments increasingly need to account for practical, technical and ethical considerations when using IoT sensors in public spaces and when managing proposals for installation and use by others. By partnering with a local council, Lancaster University's P-PITEE project, led by Dr Naomi Jacobs, helped to develop policy and guidance tools relating to the use of secure IoT sensors in public spaces. These policy and guidance tools cover collection, use and sharing of data, considerations of data transfer vs edge processing, cybersecurity questions relating to data storage and sharing, and how all these concerns can impact on privacy.

The project team used design methods to develop new policies for transparent and ethical deployment of secure Internet of Things sensors in public spaces. The team developed a novel walking workshop approach that explored and interacted with a range of speculative and real IoT and Edge computing deployments. The aim of the walking workshop was to gather understandings of how experts perceive IoT and Edge deployments in public spaces, which will help to inform the policies we are developing with the district council.

The project explores using participatory methods to engage with a variety of stakeholders including local SMEs, residents, and community groups. The project will develop a new, robust policy for ethical use of IoT data in Lancaster, research publications on interdisciplinary topics including design for technology policy and the ethical management and cybersecurity implications of public space IoT and associated data, and a fully implemented IoT Transparency Guidelines tool which can be used by organisations who are considering IoT deployments and wish to consider the transparency aspects and ethical data use.[1]

In 2022 PETRAS was successful in securing funding from EPSRC's Digital Economy 'Telling Tales of Engagement' fund to extend the participatory methods of P-PITEE as a 'train-the-trainer' offer to four further local authorities across the UK. The different levels of technical maturity and live projects within these local authorities will further inform this consultation tool and method design.

[1] PETRAS P-PITEE Project Launches TrustLens Toolkit: https://petras-iot.org/update/petras-p-pitee-project-launches-trustlens-toolkit/

PETRAS USER PARTNERS

149
OFFICIAL USER PARTNERS

39
PUBLIC SECTOR

110
INDUSTRY

OUR USER PARTNERS ARE INDUSTRY, GOVERNMENT OR PUBLIC SECTOR BODIES WHO WORK COLLABORATIVELY WITH PETRAS PROJECTS.

THEY INCLUDE:

BBC R&D
BLUESKYTEC
CONSTANTINE
CENSIS
FORESCOUT
Heathfield Ladies Residential Home
IoT Horizon Smart Solutions for the Future
IOETEC
Metrea
MIRA A HORIBA COMPANY
nquiringminds
OneWeb Low Earth Orbit Connectivity
OPENBRIX
SMARTIA
ST life.augmented
Vortex Part of Marston Holdings
IET The Institution of Engineering and Technology
YorkshireWater

INFLUENCING INDUSTRY

All PETRAS projects work with a partner from industry or government. This collaborative approach results in outcomes and impacts that emerge over the short and long term.

THE UNIVERSITY of EDINBURGH

PROJECT

Intelligible Cloud and Edge AI (ICE-AI)

TEAM

Prof Ewa Luger, Dr Bronwyn Jones, Auste Simkute with BBC R&D

Artificial Intelligence in Journalism with the BBC

Collaborative research with the BBC lead to the PETRAS' briefing 'Intelligible Cloud and Edge AI (ICE-AI) – AI and Journalism' gives an overview of artificial intelligence in journalism and focuses on how AI technologies can be applied in the news production process. By listing both the benefits and potential risks of such AI applications, the report offers a good understanding of the impact AI-driven systems can have on journalism. The briefing also summarises the challenges the adoption of AI by news organisations can have, which include laws and regulations, cost, as well as professional norms and values.

There are multiple applications of AI in journalism, primarily using machine learning techniques that learn from past data. Examples include smart systems that monitor and alert journalists to information, assist data and document analysis, automate story production and create audience profiles to drive news recommendations to them.

Key messages from the project include;

- While news organisations are using AI applications for newsgathering, production and distribution, relevant skills and technology are unequally distributed across the news industry. Future opportunities to augment journalism can emerge from machine learning and the automation of routine tasks. This could enable the improvement of the depth, diversity and appeal of news.
- Concerns have been raised relating to legal, ethical and professional implications of the use of AI in the newsroom due to issues of bias, 'black box' systems and value alignment. There are limited assessments of the impacts and implications of AI on journalism.
- More work needs to be done to avoid potential risks and ambiguities.

CARDIFF UNIVERSITY

PROJECT

Project: Resilient Built Environments (ResBE)

TEAM

Team: Dr Charith Perera and the Building Research Establishment

Secondment into Building Research Establishment (BRE)

Dr Charith Perera was seconded into Building Research Establishment (BRE) to explore resilience from a holistic viewpoint of smart office and smart home environments. With BRE, Dr Perera and his team developed a research agenda combining academic and industrial need.

They formed a better understanding on how to develop and use smart homes IoT infrastructure to gather and analyse data concerning malicious activity and anomalies and built a new smart home testbed at Cardiff University.

PROJECT

Processes for Securing Water Resource Management Systems (PSWaRMS)

TEAM

Prof Stephen Hailes, Dr Nilufer Tuptuk, Prof Tim Watson, Dr Matthew Higgins with Yorkshire Water and Nexor Ltd

Reducing the risk of cyber attack in water utilities sector

PSWaRMS investigates the existing cybersecurity processes implemented in the water utilities sector, a part of the UK's critical national infrastructure. Through close collaboration with Yorkshire Water and NEXOR, they produced a new, sector-wide, abstracted model representing the arrangement of cyber-physical assets, the role of the IoT, and the flow of data relevant to security processes. This model was validated through interactions with other water companies and stakeholders. After site tours, workshops, literature reviews and interviews to establish the foundational domain understanding for modelling, the project developed an AI-driven Situational Awareness tool capable of leveraging external and internal threat intelligence and assisting with cyber incident response. The project also developed an AI-based Randomized Target Defence approach which could reduce the risk of severe consequences from cyber-attacks aimed at the IoT assets. The project is now exploring the compatibility of these security tools for other sectors of critical national infrastructure.

PROJECT

Preventing THErmal ATtacks (PT.HEAT)

TEAM

Dr Mohamed Khamis and the Scottish Business Resilience Centre

Changes to thermal cameras help prevent cyber attacks

The PT Heat project adapted two state-of-the-art object detectors, Faster R--CNN, S and YOLO to detect vulnerable user interfaces in the feed of thermal cameras. By implementing multiple methods for obfuscating the heat traces, PT-Heat's achievements include a publicly available dataset and machine learning model; and delivery of open-source deep learning-based software through a web application and codes, currently being ported to work on thermal cameras directly by project partner CENSIS.

PROJECT

Early Anomaly Detection for Securing IoT in Industrial Automation (ELLIOTT)

TEAM

Prof Stephen Hailes, Dr Nilufer Tuptuk and Cube Control and Rockwell Automation

Early Anomaly Detection Model Protects Against Cyber Attacks

ELLIOTT has developed an AI-based early anomaly detection model. This model can be applied to industrial processes to catch early signs of cyber-attacks and thereby prevent catastrophic consequences, such as the exfiltration of sensitive data or the disruption of critical processes. The project selected the Building Automation and Control Systems sector as a use case and developed an industry-standard, hardware-in-the-loop testbed for security research at UCL. They tested the performance of this novel approach on data sets,

representing scenarios of stealthy and manual and random attacks against their testbed, as well as on other existing datasets captured from real buildings. Working with their user partner Cube Controls, they also published a set of practical guidelines on building AI-based intrusion detection systems. This was targeted towards industry practitioners as well as board-level members responsible for making decisions for securing the Internet of Things in control and automation systems.

PROJECT

Physical Graph Based Wireless IoT Security with No Key Exchange (GraphSec)

TEAM

Prof Weisi Guo, Dr Liang Wang

New security method derived from Critical National Infrastructure assets

GraphSec has developed new communication security methods, exploiting the physical information from the grid-based infrastructure, such as water, gas or electricity networks to generate decentralised and robust cipher keys. By not requiring digital key exchange, it reduces the reliance on digital attributes for security, offering widespread application for IoT systems in infrastructure monitoring. Working with wireless network deployment company Real Wireless and national infrastructure operators' group British Water, the project ensures their innovation translates to real-world impact and influences best practice.

In addition to these funded projects, PETRAS academics have benefitted from a dedicated fund of £1 million, made available under the CyberASAP Programme. More than 12 academics from across PETRAS' network were involved directly in progressing the outcome of 8 sperate projects into commercial products/services. The programme incorporates customised training & direct supports academics throughout their journey, and 5 out of the original 8 projects have now reached the stage of attracting private investments.

CYBERASAP PROJECT:

TAIMAS – Protecting your Infrastructure

TEAM

Prof Jeremy Watson, Dr Nilufer Tuptuk

PROJECT PARTNER

Tony Williams, CEO of Cube Controls Ltd.

Developing a New Method of Securing Building Management Systems (BMS) Against Cyber Attack

The CyberASAP programme funded by DCMS, provides a route for taking academic cybersecurity projects from research to early-stage commercialisation. Last year and this, an additional SDTaP funding stream has been added to CyberASAP, specifically to give PETRAS project outputs the opportunity for development towards wider-scale exploitation. TAIMAS is a project awarded under the 2021 Cohort 5. The project is a collaboration between UCL and Cube Controls Ltd.

TAIMAS is a single box solution to detect cyber-attacks and physical tampering against building management systems and industrial control systems. It is aimed at clients dissatisfied with high-cost enterprise-derived security approaches that mainly do network traffic monitoring and network attack detection. TAIMAS offers a new method independent of network traffic. Air-gapped monitoring of control system hardware utilising machine learning and both hardwired & cloud-based threat notification.

Our target market is the currently poorly protected population of legacy and newly installed building management systems in critical national infrastructure services, government, retail and hospitality. Users and operators of buildings in these sectors have immediate concerns about the adequacy of current cyber-protection measures available for their building management systems. TAIMAS will provide a cost-effective solution with a low impact, installation independent approach that ensures clients get early warning of any suspicious activity including Zero-day attacks. TAIMAS will include a range of additional optional functionalities including predictive maintenance.

PETRAS OUTREACH

Public understanding and engagement are crucial for adoption and acceptance of emerging technologies. PETRAS went about outreach in a way which created dialogue between researchers and the public; raising awareness and understanding amongst public and ensuring PETRAS research was informed by public attitudes and adoption behaviours.

EXHIBITIONS AND EVENTS

PETRAS has commissioned a number of artists to work directly with our projects and engage the public in both social and technical elements of IoT cybersecurity.

Seven artists and designers were commissioned to respond to CyFer project's research into the privacy, ethics, trust and security of female oriented technology. The "FemTech industry" remains largely unregulated. There is a lack of clarity in the law and uncertainty concerning industry and user practice in relation to this extremely sensitive data on different levels i.e. user consent, third-party sharing, and algorithmic bias which may lead to malicious purposes. Engaging artists and designers in this way allowed the public to explore the research in a way which technical understanding, social implications, feelings and emotions could be entangled, reflecting the true complexity of IoT deployment and development. The works will be exhibited in high profile galleries throughout the summer of 2023 and have contributed to PETRAS's contribution to Mozilla Festival 2023.

PETRAS has ensured that it took research to the public:

- Edge of Reality ran interactive experiences in their caravan of the future at Liverpool World Museum, the V&A and on Leicester High Street as part of British Science Festival 2022
- ICE-AI allowed the public to experience producing news reports with the support of AI at Edinburgh Science Festival 2023
- Over 500 school children explored the sustainability of IoT through Edge of Reality's Prometheus game at Cheltenham Science Festival
- and, in December 2022, older adults from across Edinburgh designed the IoT they want to see as part of the Hack Your Age project

PETRAS CENTRE EVENTS AND COMMUNICATION (FROM 2019 ONWARDS)

8
USER RESEARCH BOARDS

6
OUTREACH EVENTS

7
PUBLIC EVENTS AIMED AT INDUSTRY GOVERNMENT AND ACADEMIC ENGAGEMENT

25
PETRAS COMMUNITY DEVELOPMENT EVENTS

3
ONLINE COLLABORATION WITH IET EVENTS

3
INDUSTRY ENGAGEMENT EVENTS

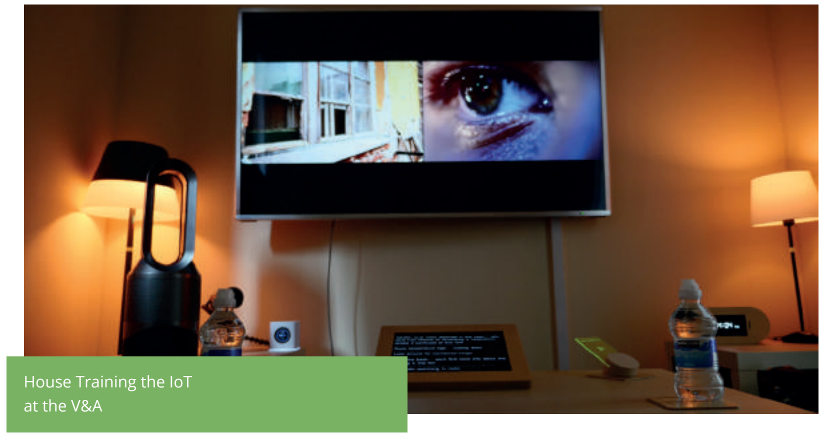
8
WORKSHOPS AND ROUNDTABLES

510
510 SUBSCRIBERS IN ACADEMIA, GOVERNMENT AND INDUSTRY, FOR 46+ NEWSLETTERS

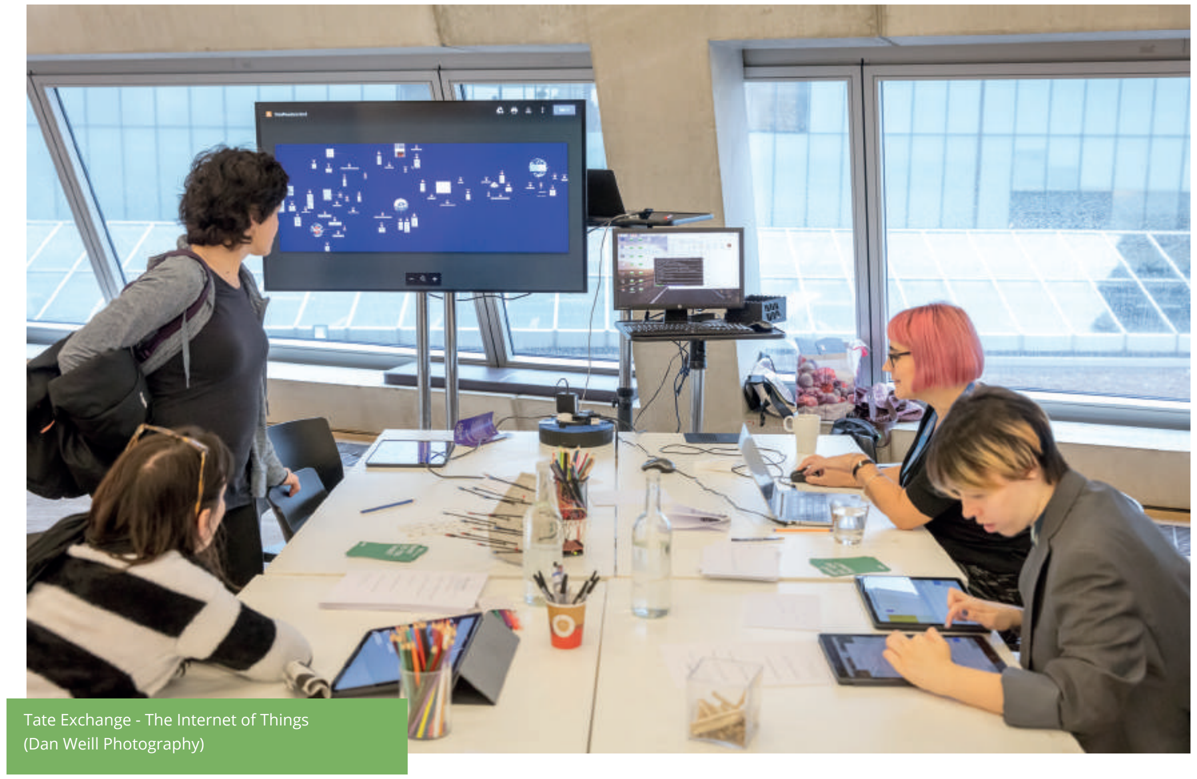
3400
DELEGATES IN TOTAL

Tate Exchange - The Internet of Things
(Dan Weill Photography)

Tate Exchange - The Internet of Things
(Dan Weill Photography)



House Training the IoT
at the V&A



Tate Exchange - The Internet of Things
(Dan Weill Photography)

1st International Workshop on Socio-technical Cybersecurity and Resilience in the Internet of Things

PECKHAM PLATFORM
PEOPLE UNITED
PEOPLE'S BUREAU
PLYMOUTH COLLEGE OF ART
PUBLIC WORKS
QUEEN MARY UNIVERSITY OF LONDON
ROOM 13 HAREHILLS BRISTOL
ROYAL HOLLOWAY AND BEDFORD NEW COLLEGE LONDON

Tate Exchange - The Internet of Things
(Dan Weill Photography)

PODCAST SERIES

The PETRAS National Centre of Excellence for IoT Systems Cybersecurity's 'At the Edge' first podcast series responded to Cop26 by exploring how the Internet of Things (IoT), AI and cybersecurity technologies may help (or hinder?) humanity with its greatest challenges of tackling climate change and achieving Net Zero targets.

Each episode comprised of a lively and engaging conversation between experts from across academia, industry and government. Discussions ranged from the need for greater cybersecurity awareness in our food supply chains and the more (and less) sustainable behaviours "smart cities" may encourage, to the role IoT plays in sustainable energy transitions and whether IoT favours the poachers or the poached in the context of wildlife conservation;

This series has been listened to 530 times and continues to receive new downloads.

The second podcast series will be released in April 2023 and focus on secure connected places. Episodes explore the way in which local authorities, national government, the public sector and industry can most successfully collaborate to deliver secure connected places; the role of IoT in delivering healthy and happy places of the future; whether the public trust mobility as a service; and how local authorities consider the ethics of IoT when evaluating deployments.

We have been delighted to host guests from our many partners including: Siemens, SOCITM, Toshiba, DSIT, London Zoo and The Connected Places Catapult.

The podcast series is available via all major podcast platforms including:

- Apple
- Spotify
- Google Podcasts

PETRAS PUBLICATIONS

PETRAS Reseach Knowledge Base

You can explore PETRAS's Research Knowledge Base of peer reviewed, multidisciplinary publications at this link:

https://petras-iot.org/petraspublications/

As the technological and societal context constantly changes and evolves, so does the evidence base. Enhanced understanding and insights are being developed all the time and new solutions proposed. Therefore, even the best evidence gathered will only be a snapshot in time, quickly superseded by the next project or report.

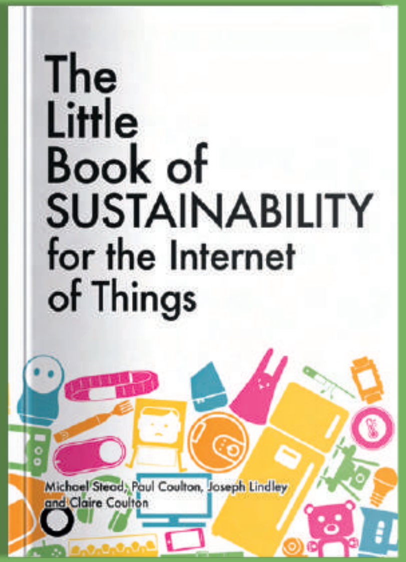
Nevertheless, in this constantly shifting, fast paced environment, it is important to have a legacy repository of work that can be easily accessed, navigated and built upon.

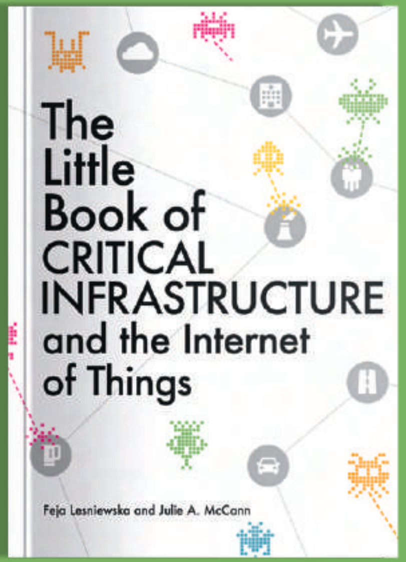
As well as academic peer reviewed publications, PETRAS produces publications for non-academic audiences, including landscape reviews, policy briefings, white papers and tools for industry and local government.

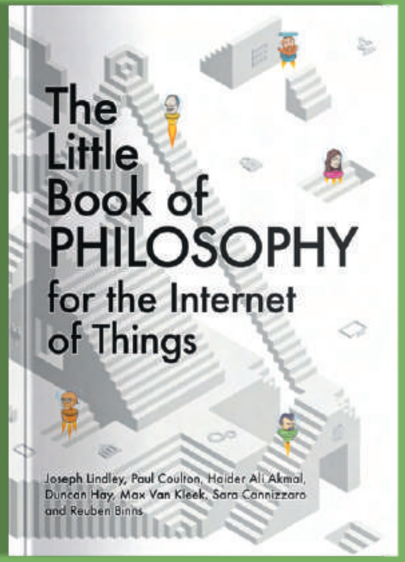
Little Books Series https://petras-iot.org/update/petras-little-book-series-to-engage-wide-audience/

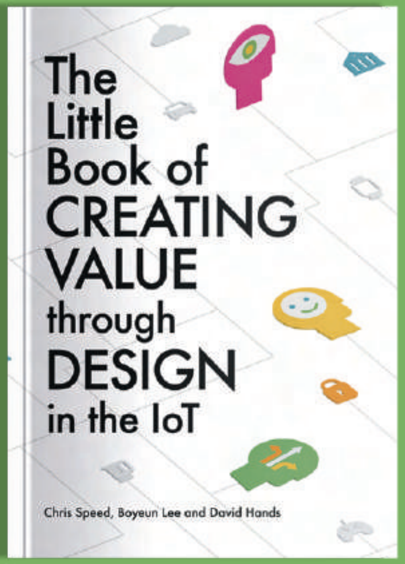
Landscape Briefing series https://petras-iot.org/update/covid-19-the-internet-of-things-and-cybersecurity/

Industry Briefings https://petras-iot.org/update/petras-industry-briefings/

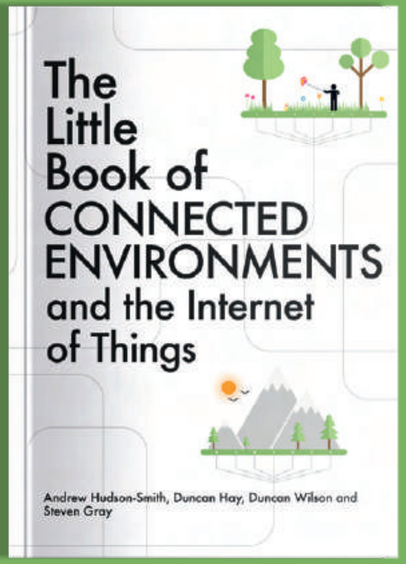

The Little Book of SUSTAINABILITY for the Internet of Things
Michael Stead, Paul Coulton, Joseph Lindley and Claire Coulton

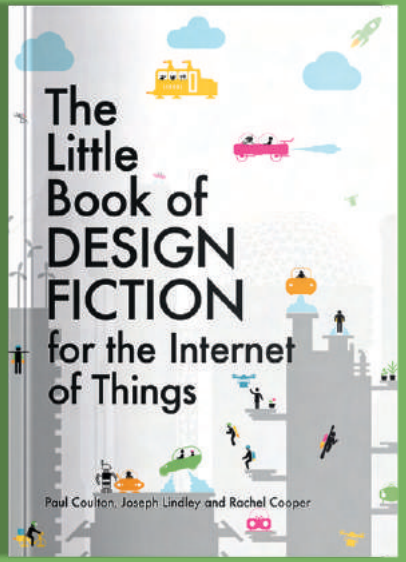

The Little Book of CRITICAL INFRASTRUCTURE and the Internet of Things
Feja Lesniewska and Julie A. McCann


The Little Book of PHILOSOPHY for the Internet of Things
Joseph Lindley, Paul Coulton, Haider Ali Akmal, Duncan Hay, Max Van Kleek, Sara Cannizzaro and Reuben Binns


The Little Book of CREATING VALUE through DESIGN in the IoT
Chris Speed, Boyeun Lee and David Hands

The Little Book of the Internet of Things for the HOME
Adrian Gradinar, Max Van Kleek, Larissa Pschetz
Paul Coulton and Joseph Lindley


The Little Book of CONNECTED ENVIRONMENTS and the Internet of Things
Andrew Hudson-Smith, Duncan Hay, Duncan Wilson and Steven Gray


The Little Book of DESIGN FICTION for the Internet of Things
Paul Coulton, Joseph Lindley and Rachel Cooper

PETRAS LEGACY

NEXT GENERATION OF RESEARCHERS

PETRAS postdoctoral researchers and funded PhD students have been highly successful in their careers post PETRAS. 11+ postdocs have now gone on to lectureships while two have been awarded FutureLeaders Fellowships (Joe Lindley and Leonie Tanczer). Those who have moved on to lectureships have been successful in developing their own research agendas, often building on research from their early PETRAS work. PETRAS postdoctoral researchers also have the skills that are increasingly valued in industrial sectors, with a number going into jobs in the security sector, and on secondment to Government departments where their skills have had direct impact on policy.

DR IRINA BRASS

ASSOCIATE PROFESSOR, UCL DEPARTMENT OF SCIENCE, TECHNOLOGY, ENGINEERING AND PUBLIC POLICY

Dr Irina Brass, with a research background in standards and regulation of emerging technologies, joined PETRAS in 2016 as Postdoctoral Research Associate (PDRA), before being promoted to Co-Investigator. In October 2016, the Mirai botnet attack occurred and soon after, the HMG Department for Digital, Culture, Media and Sports (DCMS) launched a joint review with NCSC to identify proposals for improving the cyber security of consumer IoT products and associated services.

Dr Brass joined the DCMS expert advisory group that later informed the development of a Code of Practice for Consumer IoT Security and presented to the IoT-1 Technical Committee at BSI – the UK's National Standards Body, making a strong case for the development of horizontal standards that promote a responsible baseline for IoT security and privacy. She soon became the Chair of the BSI IoT-1 Committee and was then appointed member of the Standards Policy and Strategy Committee (SPSC), which advises the BSI Board of Directors on the development of future British Standards.

Dr Brass continues her research on the ways in which regulation and standards can be co-developed to keep pace with the emerging risks associated with digital technologies such as the IoT. In 2021, she co-authored a paper on the creation of more adaptive governance models for IoT, published in the prestigious "Regulation & Governance" Journal.

Dr Brass leads the PETRAS Reg-MedTech1 project which investigates the standards and regulatory changes needed to address critical cybersecurity and algorithmic trustworthiness issues in connected, intelligent medical devices. Working in partnership with BSI, the Reg-MedTech project produced a mapping tool of standards relevant to the Internet of Medical Things (IoMT) and a White Paper highlighting several priority areas for updating existing regulations and guidelines applicable to software-based medical devices or software as a medical device. The Reg-MedTech project also convened a workshop with medical and healthcare professionals interacting with the IoMT, which addressed the main challenges they are facing when providing patient care facilitated by emerging digital technologies and the best ways they can be supported with training, guidance, and institutional changes to minimise digital technologies risks in the healthcare setting.

1. https://petras-iot.org/project/regulatory-and-standardization-challenges-for-connected-and-intelligent-medical-devices-reg-medtech/

DR UCHENNA ANI

LECTURER IN CYBER SECURITY, SCHOOL OF COMPUTER SCIENCE AND MATHEMATICS, KEELE UNIVERSITY

Dr Ani obtained his first degree in Computer Science and his Master's Degree in Computer Security and Forensics from the University of Bedfordshire, UK, and took up the role of Lecturer in Computer Science at Federal University Lokoja, Nigeria. Dr Ani later went on to complete a PhD in Industrial Control System Cybersecurity at Cranfield University, UK.

Dr Ani was a Senior Research Fellow in Cybersecurity at the PETRAS National Centre of Excellence for IoT Systems Cybersecurity at the Department of Science Technology Engineering and Public Policy (STEaPP), University College London (UCL). He was involved in leading and guiding the direction of some of the IoT-enabled critical infrastructure security projects in the PETRAS Centre Consortium.

For example, PETRAS CoSTCMoRS project is developing a hybrid and adaptive approach to combining AI and a socio-technical model to identify and detect cyberattacks and create a holistic & fast response to cyber incidents to ensure the security, safety, and functionality of a modern railway system (MRS).

Through Dr Ani, the project has input into the Key Train Requirement (KTR) group since November 2021. Contributing to the development of the KTR document is crucial because it raises awareness both in industrial spheres as well as in governmental departments of the importance of including cybersecurity considerations in standards and initiatives.

Since 2022, Dr Ani leads the MSc. Cyber Security programme in the School of Computer Science and Mathematics at Keele University. He is a Fellow of the Higher Education Academy (FHEA), a Member of the Institution of Engineering and Technology (IET), a Member of the Association of Computing Machinery (ACM). He is a School Taught Programme Ethics Committee Chair.

[1] Petras - Cognitive and Socio-Technical Cybersecurity in Modern Railway System (CoSTCMoRS) https://petras-iot.org/project/cognitive-and-socio-technical-cybersecurity-in-modern-railway-system-costcmors/

DR JOE LINDLEY

SENIOR RESEARCH FELLOW, IMAGINATIONLANCASTER, LANCASTER UNIVERSITY

Dr Lindley is currently a UKRI Future Leaders Fellow running a £1.2m 4-year project titled Design Research Works[1]. The main objective of the project is to show the world the value of Design-led approaches to understanding the socio-technological opportunities posed by emerging tech such as the Internet of Things and Artificial Intelligence. This extends on work conducted with PETRAS.

During nearly 4-years with PETRAS Dr Lindley was a Postdoctoral Research Associate whose role was to explore the adoption and acceptability of emerging technologies. Dr Lindley's approach built on his doctoral research and utilised the Design Fiction as World Building, creating prototypes that delve into known acceptability challenges and propose possible adoption solutions. This research has been presented at government departments, consumer rights organisations, as well as world-leading art venues and academic conferences.

Dr Lindley's PETRAS research, conducted in collaboration with Professor Paul Coulton, has contributed to a More-than-Human turn in Design. This movement embraces the need to update long-held notions of human-centred design. Human-centred design needs to be reconsidered in order to respond to the 21st centuries complexities and represent individual needs alongside societal, economic, and environmental considerations.

Insights arising from Dr Lindley's research have been included in two submissions to the UK Government including the Parliamentary Inquiry on Governance of Artificial Intelligence[2], he was a co-author of Advancing ethics review practices in AI research published by Nature in 2023[3], he is alumnus of the ACM Future of Computing Academy[4], and is an active member of the Responsible AI Licensing initiative.

[1] https://designresearch.works/

[2] See https://kclpure.kcl.ac.uk/portal/files/175710766/Call_for_evidence_Parliamentary_inquiry_FINAL_2.pdf and https://doi.org/10.18742/pub01-104

[3] https://www.nature.com/articles/s42256-022-00585-2

[4] https://medium.com/acmfca/goodbye-fca-9cce1c87d6ee

INFLUENCING THE RESEARCH LANDSCAPE

PETRAS' academic influence continues to grow both nationally and internationally. For example, approximately 45% of PETRAS research publications between 2016–2022 has at least 10 citations and 30% of PETRAS publications are considered highly impactful (ML Model of Semantic Scholar). Research also reveals that we have connections through these publications to 813 researchers across academia, Research Centres, Industries and Businesses both nationally and internationally.

PETRAS academics have been instrumental in informing national and international research agendas and funding. For example, PETRAS input academic expertise to the development of the Digital Footprints programme[1], ensured that IoT data was included in the research scope, as opposed to only focusing on social media data and thus expanded the research scope of the programme. Another PETRAS academic initiative received funding from the Welsh Government and Cardiff Capital Region to create the £13.8m Cyber Innovation Centre[2] building on work from the PETRAS programme.

[1] The aim of the Digital Footprints programme is to coordinate, convene, develop and support thriving interdisciplinary digital footprint data communities, focused on addressing pressing national and international challenges. The programme will be delivered in 2 phases. The budget is a total of £59.3 million between 2022 and 2029. Phase 1 will run from 2022 to 2024. Phase 2 will run from 2023 to 2029

[2] For further information see https://cyberinnovationhub.wales/challenge-call-february-2023

1st International Workshop on Socio-technical Cybersecurity and Resilience in the Internet of Things

STAR-IOT

1ST INTERNATIONAL WORKSHOP ON SOCIO-TECHNICAL CYBERSECURITY AND RESILIENCE, DELFT, NETHERLANDS

In November 2022, PETRAS chaired the 1st International Workshop on Socio-technical Cybersecurity and Resilience in the Internet of Things; hosted within the 12th International Conference of the Internet of Things at the Faculty of Industrial Design Engineering (IDE), on the TU Delft campus in the Netherlands.

The focus of the workshop was to demonstrate that IoT and modern networks can increase security, safety, and resilience when used well. The workshop brought together socio-technical researchers to better understand safe and resilient IoT systems, in a way that is culturally appropriate and ethically acceptable and that breeds, rather than subverts, confidence.

This workshop considered research that examined both social and technical issues relating to the resilience and cybersecurity of IoT devices, systems, and networks. It brought together researchers to discuss socio-technical challenges and opportunities of IoT technologies, multi-scale deployments of embedded technologies in smart cities, Industry 4.0, logistics, etc.

It compared local and international regulation, standardization and certification, and public trust in such technologies, and examined the cybersecurity and resilience of dual-use technologies. This research informed cybersecurity of critical infrastructure, resilience and current geopolitical challenges, international alliances and collaboration, supply-chain security, and preparedness.

Faculty of Industrial Design Engineering (IDE), on the TU Delft campus in the Netherlands.

UP TO 2023, PETRAS ACADEMICS HAVE PUBLISHED:

213

Journal Articles

33

Books (incl. contributions and chapters etc)

190

Conferences and Proceedings

15+

White Papers, Policy Briefings and Reports

11

Landscape Briefings
https://petras-iot.org/update/covid-19-the-internet-of-things-and-cybersecurity/

6+

sector specific Industry Briefings
https://petras-iot.org/update/petras-industry-briefings/

12

Podcast (with over 500 listeners)

45%

Of PETRAS research publications between 2016–2022 has at least 10 citations

30%

Of PETRAS publications are considered highly impactful (ML Model of Semantic Scholar)

813

PETRAS connections through these publications to researchers across academia, research centres, industries and businesses both nationally and internationally.

PETRAS PROJECTS

Below you will find a full list of all the PETRAS projects along with the URL where you can find further information.

PETRAS Project Title	University	Sector	Project Team	URL
Cybersecurity for Food Security (CyFoo)	University of Bristol	Agritech	Prof Awais Rashid, Dr Barney Craggs, Sharad Agarwal, Joe Gardiner	**https://petras-iot.org/project/cybersecurity-for-food-security-cyfoo-2/**
Formal methods for Agritech Resilience Modelling (formerly named "Hierarchical Modelling & Verification for Resilient Agritech (FARM)	University of Glasgow	Agritech	Dr Michele Sevegnani, Dr Yue Gu	**https://petras-iot.org/project/formal-methods-for-agritech-resilience-modelling-farm/**
Building Public Value via Intelligible AI (PubVIA)	University of Edinburgh	Ambient Environments	Dr Bronwyn Jones, Prof Ewa Luger, Dr Chris Elsden	**https://petras-iot.org/project/building-public-value-via-intelligible-ai-pubvia/**
Child Proofing the Internet of Things (IoT4Kids)	Lancaster University	Ambient Environments	Dr Bran Knowles, Dr Joe Finney	**https://petras-iot.org/publication/iot4kids-strategies-for-mitigating-against-risks-of-iot-for-children/**
Demonstration of a Secure, Low- Power tracking system for works of art (Art Connect)	Imperial College London	Ambient Environments	Prof Julie McCann	**https://petras-iot.org/update/petras-demonstrators-bringing-research-into-the-real-world/**
Displays and Sensors on Smart Campus (DiSSC)	University of Lancaster, University of Surrey	Ambient Environments	Prof Nigel Davies, Prof Paul Coulton, Dr Mateusz Mikusz, Prof Klaus Moessner, Dr Haitham Cruickshank	**https://petras-iot.org/project/displays-and-sensors-on-smart-campuses-dissc/**
Edge of Reality (ER)	Lancaster University	Ambient Environments	Dr Mike Stead, Dr Adrian Gradinar, Fran Pilling, Dr Matthew Pilling, Prof Paul Coulton	**https://petras-iot.org/project/edge-of-reality-er/**
Edge of Tomorrow: Understanding the Impacts of IoT XCybersecurity and Datafication to Co-design a Sustainable Edge (ET)	Lancaster University	Ambient Environments	Dr Mike Stead, Dr Adrian Gradinar, Fran Pilling	**https://petras-iot.org/project/edge-of-tomorrow-understanding-the-impacts-of-iot-cybersecurity-and-datafication-to-co-design-a-sustainable-edge-et/**
Evaluating Trustworthiness of Edge-Based Multi-Tenanted IoT Devices (TEAM)	University of Warwick	Ambient Environments	Dr Arshad Jhumka, Dr Matthew Bradbury	**https://petras-iot.org/project/evaluating-trustworthiness-of-edge-based-multi-tenanted-iot-devices-team/**
Evaluation of IoT Systems' Requirements for Tracking Applications (Things d'Art)	Imperial College London	Ambient Environments	Prof. Julie McCann, Dr Roman Kolcun	**https://petras-iot.org/project/evaluation-of-iot-systems-requirements-for-tracking-applications-things-dart/**
Experimental IoT: Explorations in Sound Art and Technology (EXIoT)	University of Nottingham	Ambient Environments	Dr Alan Chamberlain, Prof Dave de Roure	**https://petras-iot.org/project/experimental-iot-explorations-in-sound-art-and-technology-exiot/**
House Training the Internet of Things (HTIoT)	Lancaster University	Ambient Environments	Prof Paul Coulton, Dr Joe Lindely	**https://petras-iot.org/project/house-training-the-internet-of-things-htiot/**
Intelligible Cloud and Edge AI (ICE-AI)	University of Edinburgh	Ambient Environments	Prof Ewa Luger, Dr Bronwyn Jones, Auste Simkute	**https://petras-iot.org/project/intelligible-cloud-and-edge-ai-ice-ai/**
IoT in the Home (IoTitH)	University College London	Ambient Environments	Prof. Jeremy Watson	**https://petras-iot.org/update/iot-in-the-home-demonstrator/**
IoT in the Park: Queen Elizabeth Olympic Park Demonstrator	University College London/ Imperial College London	Ambient Environments	Prof Andy Hudson-Smith/ Prof Julie McCann	**https://petras-iot.org/project/iot-in-the-park/**
IoT of Trees (IoToT)	University College London	Ambient Environments	Prof. Andy Hudson-Smith	**https://petras-iot.org/project/iot-of-trees-iotot/**
Making the Invisible Visible - Secure, Trustworthy IoT Displays and Sensors for Urban Environments in CityVerve (IDice)	Lancaster University	Ambient Environments	Prof Nigel Davies	**https://petras-iot.org/project/making-the-invisible-visible-secure-trustworthy-iot-displays-and-sensors-for-urban-environments-in-cityverve-idice/**
Managing Access to Smart Building Information (MASBI)	Newcastle University	Ambient Environments	Dr Charles Morisset	**https://petras-iot.org/update/petras-demonstrators-bringing-research-into-the-real-world/**
Markets for Connected Space Sharing (MaCs)	University of Newcastle	Ambient Environments	Dr Charles Morisset, Prof Lilian Edwards, Rima Alaaeddine, Charles Neu, Natalie Leesakul	**https://petras-iot.org/project/markets-for-connected-space-sharing-macs/**
New forms of Public Value at the Edge: Designing for HDI and Trust in Media IoT Futures (eValuatE)	University of Nottingham	Ambient Environments	Prof Derek Macauley, Dr Neelima Sailaja, Dr Richard Ramchurn	**https://petras-iot.org/project/new-forms-of-public-value-at-the-edge-designing-for-hdi-and-trust-in-media-iot-futures-evaluate/**
Participatory Policies for IoT (P-PITEE)	Lancaster University	Ambient Environments	Dr Naomi Jacobs, Dr Lou Mullagh	**https://petras-iot.org/project/participatory-policies-for-iot-at-the-edge-ethics-p-pitee/**

PETRAS Project Title	University	Sector	Project Team	URL
Preventing THErmal Attacks (PT.HEAT)	University of Glasgow	Ambient Environments	Dr Mohamed Khamis, Shaun Macdonald	**https://petras-iot.org/project/preventing-thermal-attacks-pt-heat/**
Privacy-Preserving Indoor Environment Monitoring (PPIEM)	University of Newcastle	Ambient Environments	Dr Charles Morisset, Prof Lilian Edwards, Charles Neu, Natalie Leesakul	**https://petras-iot.org/project/privacy-preserving-indoor-environment-monitoring-ppiem/**
Resilient Built Environments (ResBE)	University of Cardiff	Ambient Environments	Dr Charith Perera	**https://petras-iot.org/project/resilient-built-environments-resbe/**
Resolving Conflicts in Public Spaces (ReCoPS)	University of Surrey	Ambient Environments	Prof Klaus Moessner	**https://petras-iot.org/project/resolving-conflicts-in-public-spaces-recops/**
Respectful Things in Private Spaces: Investigating Ethical Data Handling for Very Personal Devices (ReTiPS)	University of Oxford	Ambient Environments	Prof. Sir N. Shadbolt	**https://petras-iot.org/project/respectful-things-in-private-spaces-retips/**
Roadmap for the Internet of Things in Queen Elizabeth Olympic Park (aRIoT)	University College London	Ambient Environments	Dr Duncan Hay	**https://petras-iot.org/project/a-roadmap-for-the-internet-of-things-in-queen-elizabeth-olympic-park-ariot/**
Secure Payments in Smart Environments (SPiSE)	University of Oxford	Ambient Environments	Prof Ivan Martinovic, Simon Birnback, Dr Simon Eberz	**https://petras-iot.org/project/secure-payments-in-smart-environments-spise/**
Securing the Value of Smart Metering (SeMIoT)	Imperial College London	Ambient Environments	Dr Pantelis Koutroumpis	**https://petras-iot.org/project/securing-the-value-of-smart-metering-semiot/**
Smart Transaction in Public Spaces (STiPS)	University of Edinburgh	Ambient Environments	Prof Chris Speed, Dr Ella Tallyn	**https://petras-iot.org/update/stips-in-the-wild/**
The Reappearing Computer: Foregrounding Privacy in IoT (REAPPEAR)	University of Newcastle	Ambient Environments	Dr Nick Taylor, Dr Dave Chatting, Prof Jayne Wallace, Prof Jon Rogers	**https://petras-iot.org/project/the-reappearing-computer-foregrounding-privacy-in-iot-reappear/**
The Responding to Attacks and Compromise at the Edge (RACE)	Imperial College London	Ambient Environments	Prof Emil Lupo, Dr Marwa Salayma	**https://petras-iot.org/project/responding-to-attacks-and-compromise-at-the-edge-race/**
Trust and Privacy as Design Principles for IoT Infrastructures (DePrIoT)	University of Oxford	Ambient Environments	Prof Mariarosaria Taddeo, Prof Luciano Floridi, Prof Sandra Wachter	**https://petras-iot.org/project/trust-and-privacy-as-design-principles-for-iot-infrastructures-depriot/**
Understanding and Mitigating Privacy risks of IoT Homes with Demand-Side Management (PrivIoT)	Northumbria University	Ambient Environments	Dr James Nicholson, Dr Stefanie Kuenzel, Dr David Buil-Gil, Rhian Lukins	**https://petras-iot.org/project/understanding-and-mitigating-privacy-risks-of-iot-homes-with-demand-side-management-priviot/**
User-Centric Design for Adoption of IoT (UDAIoT)	University of Warwick	Ambient Environments	Dr Anya Skatova, Rob Procter, Dr Arkaitz Zubiaga	**https://petras-iot.org/project/user-centric-design-for-adoption-of-iot-udaiot/**
Value of Personal Data in IoT (VPD)	University of Warwick	Ambient Environments	Dr A. Skatova, Prof. C. Maple	**https://petras-iot.org/project/value-of-personal-data-in-iot-vpd/**
IoT in the Home (IoTitH)	University College London	Ambient Environments	Prof. Jeremy Watson	**https://petras-iot.org/update/iot-in-the-home-demonstrator/**
Demonstration of a Secure, Low- Power tracking system for works of art (Art Connect)	Imperial College London	Ambient Environments	Prof Julie McCann	**https://petras-iot.org/update/petras-demonstrators-bringing-research-into-the-real-world/**
IoT in the Park: Queen Elizabeth Olympic Park Demonstrator	University College London/ Imperial College London	Ambient Environments	Prof Andy Hudson-Smith/ Prof Julie McCann	**https://petras-iot.org/update/petras-demonstrators-bringing-research-into-the-real-world/**
Managing Access to Smart Building Information (MASBI)	Newcastle University	Ambient Environments	Dr Charles Morisset	**https://petras-iot.org/project/iot-in-the-park/**
Authentication & Access Control through Multiple IoT Devices (AACIoT)	University of Warwick	Health and Wellbeing	Prof Carsten Maple, Dr Hu Yuan	**https://petras-iot.org/project/authentication-and-access-control-with-multiple-iot-devices-aaciot/**
Building Evident base for CoP Legislation(BECL)	University College London	Health and Wellbeing	Dr Saheli Datta Burton, Nicholas Zuniga, Daniel Rojas Lozano	**https://petras-iot.org/project/building-evidence-base-for-cop-legislation-becl/**
Cyber Security and privacy in Fertility Technologies (CyFer)	University of Newcastle	Health and Wellbeing	Dr Maryam Mehrnezhad, Dr Eshas Toreini	**https://petras-iot.org/project/cyber-security-and-privacy-in-fertility-technologies-cyfer/**
Cyberphysical Social Machines (CP-SOCIAM)	University of Southampton	Health and Wellbeing	Dame Wendy Hall, Dr Paul Smart	**https://petras-iot.org/project/cp-sociam/**
Data Analysis and IoT Solutions for Healthcare (DASH)	University of Oxford	Health and Wellbeing	Prof Mariarosaria Taddeo, Prof Luciano Floridi, and Prof Brent Mittelstadt	**https://petras-iot.org/project/data-analysis-and-iot-solutions-for-healthcare-dash/**
Health IoT Privacy & Security Transferred to Engineering Requirements (HIPSTER)	Lancaster University	Health and Wellbeing	Prof Dan Prince, Dr Charles Weir, Dr Anna Dyson	**https://petras-iot.org/project/health-iot-privacy-and-security-transferred-to-engineering-requirements-hipster/**

PETRAS Project Title	University	Sector	Project Team	URL
Hybrid Engagement Architecture Layer for Trusted Human-Centric IoT (HEALTH-I)	University of Southampton	Health and Wellbeing	Dame Wendy Hall	**https://petras-iot.org/project/health-i-hybrid-engagement-architecture-layer-for-trusted-human-centric-iot/**
IoT Security for Healthcare (SeNTH +)	Imperial College London	Health and Wellbeing	Prof. G-Z. Yang	**https://petras-iot.org/project/security-and-new-threats-in-healthcare-senth/**
Privacy Preserving IoT Security Management (PRISM)	Imperial College London	Health and Wellbeing	Dr Hamed Haddadi, Dr Anna Maria Mandalari	**https://petras-iot.org/project/privacy-preserving-iot-security-management-prism/**
Privacy-Enhancing and Identification-Enabling Solutions for IoT (PEIESI)	University of Oxford	Health and Wellbeing	Prof Mariarosaria Taddeo, Prof Luciano Floridi, Prof Sandra Wachter	**https://petras-iot.org/project/privacy-enhancing-and-identification-enabling-iot-solutions-peiesi/**
Privacy-preserving Data Sharing and Trading Ecosystem for Distributed Wireless IoT Networks (PRISTINE)	University of Glasgow	Health and Wellbeing	Dr Lei Zang, Prof Cathy Yi-Hsuan Chen, Prof Simon Joss, Prof Muhammad Ali Imran, Dr Xiaoshuai Zhang	**https://petras-iot.org/project/privacy-preserving-data-sharing-and-trading-ecosystem-for-distributed-wireless-iot-networks-pristine/**
Regulatory and Standardisation Challenges for Connected an Intelligent Medical Devices (REG-MEDTECH)	University College London	Health and Wellbeing	Dr Irina Brass, Dr Jesse Sowell, Dr Andrew Mkwashi, Dr Isabel Straw	**https://petras-iot.org/project/regulatory-and-standardization-challenges-for-connected-and-intelligent-medical-devices-reg-medtech/**
REspectful and capability-centreD AI Device for Preventing Call Fraud (Red-AID)	University of Oxford	Health and Wellbeing	Prof Max Van Kleek, Dr Peter Novitzky	**https://petras-iot.org/project/red-aid-respectful-and-capability-centred-ai-device-for-preventing-call-fraud/**
Security & New Threats in Healthcare (SeNTH)	Imperial College London	Health and Wellbeing	Dr Charence Wong, Prof Guang-Zhong Yang, Dr Benny Lo, Prof Emil Lupu	**https://petras-iot.org/project/lightweight-security-and-privacy-for-geographic-personal-data-and-location-based-services-geosec/**
Analytical Lenses for IoT Threats (AlloTT)	University College London, University of Warwick	Infrastructure	Prof Jeremy Watson, Prof Carsten Maple	**https://petras-iot.org/project/analytical-lenses-for-iot-threats-aliott/**
Authentication & Access Control through Multiple IoT Devices (IoTinControl)	University College London, University of Bristol, University of Warwick	Infrastructure	Prof Stephen Hailes, Prof Awais Rashid, Prof Carsten Maple	**https://petras-iot.org/project/iot-in-control/**
Blockchain-empowered Infrastructure for IoT (BlockIT)	University of Southampton	Infrastructure	Prof. W. Hall and Prof. V. Sassone	**https://petras-iot.org/project/blockchain-empowered-infrastructure-for-iot-blockit/**
Bridging the gap between legal and technical anonymisation (BLATA)	Imperial College London	Infrastructure	Dr Yves-Alexandre de Montjoye, Dr Andrea Gadotti	**https://petras-iot.org/project/bridging-the-gap-between-legal-and-technical-anonymisation/**
Cloudlet Enhances Devices at the Edge (CEDE)	Lancaster Lancaster	Infrastructure	Prof Nigel Davies, Dr Mike Harding, Peter Shaw	**https://petras-iot.org/project/cloudlet-enhanced-devices-at-the-edge-cede/**
Cyber Risk Assessment for Coupled Systems (CRACS)	University of Oxford	Infrastructure	Dr Jason Nurse, Prof Sadie Creese, Prof Dave de Roure	**https://petras-iot.org/project/cyber-risk-assessment-for-coupled-systems-cracs/**
Cyber Security of IoT in Critical National Infrastructure (IoTinCNI)	University of Bristol	Infrastructure	Prof Awais Rashid	**https://petras-iot.org/project/cyber-security-of-iot-in-critical-national-infrastructure-iotincni/**
Developing a Consumer Security Index for Domestic IoT devices (CSI)	University College London	Infrastructure	Prof. S. Johnson	**https://petras-iot.org/project/developing-a-consumer-security-index-for-consumer-iot-devices-csi/**
Developing a Consumer Security Index for Domestic IoT devices Plus (CSI+)	University College London	Infrastructure	Prof. S. Johnson	**https://petras-iot.org/project/developing-a-consumer-security-index-for-domestic-iot-devices-plus-csi/**
Digital Twins in Cyber Effects Modelling of Iot/ CPS Points of Low Resilience (DTCEM)	University of Warwick	Infrastructure	Dr Gregory Epiphaniou, Prof Carsten Maple, Dr Mohammad Hammoudeh	**https://petras-iot.org/project/digital-twins-in-cyber-effects-modelling-of-iot-cps-points-of-low-resilience-dtcem/**
Future Infrastructure for Retail Remittances (FIRE)	University College London/ University of Edinburgh	Infrastructure	Prof Tomaso Aste, Dr Geoffrey Goodell, Prof Chris Speed	**https://petras-iot.org/project/future-infrastructure-for-retail-remittances-fire/**
Geopolitics of IIoT Standards (GISt)	University College London	Infrastructure	Prof Madeline Carr, Dr Saheli Datta Burton, Nick Zuniga	**https://petras-iot.org/project/geopolitics-of-iiot-standards-gist/**
Home Area Network Code of Practice (HANCODE)	University of Warwick	Infrastructure	Hugh Boyes, Prof Carsten Maple	**https://petras-iot.org/project/home-area-network-code-of-practice-hancode/**
Integrated Cyber-Secure Edge Computing (ICEC)	University of Oxford	Infrastructure	Prof Dave de Roure, Dr Petar Radanliev	**https://petras-iot.org/project/integrated-cyber-secure-edge-computing-icec/**
IoT Multidisciplinary Standards Platform (IoT MSP)	University College London	Infrastructure	Dr Rob Thompson, Graça Carvalho, Prof Jeremy Watson	**https://petras-iot.org/project/iot-multi-disciplinary-standards-platform-iotmsp/**

PETRAS Project Title	University	Sector	Project Team	URL
IoT Observatory	University of Southampton	Infrastructure	Dame Wendy Hall, Prof Thanassis Tiropanis, Dr Aastha Madaan, Dr Xin Wang	**https://petras-iot.org/project/iot-observatory/**
Modelling the potential impact of IoT boosted botnet attacks (BotThings)	University College London	Infrastructure	Dr G. Stringhini	**https://petras-iot.org/project/botthings/**
National & International Policy for Critical Infrastructure Cybersecurity (NiPC)	University College London	Infrastructure	Prof Madeline Carr, Dr Feja Lesniewska	**https://petras-iot.org/project/national-and-international-policy-for-critical-infrastructure-cybersecurity-nipc/**
PETRAS-IoT Data Management and Sharing Infrastructure: An Evolution of IoT Observatory (PEDASI)	University of Southampton	Infrastructure	Dame Wendy Hall	**https://petras-iot.org/update/petras-demonstrators-bringing-research-into-the-real-world/**
Physical Graph Based Wireless IoT Security with No Key Exchange (GraphSec)	Cranfield University	Infrastructure	Prof Weisi Guo, Dr Liang Wang	**https://petras-iot.org/project/physical-graph-based-wireless-iot-security-with-no-key-exchange-graphsec/**
Positional Referencing for IoT at the Edge (PRIoTE)	University of Warwick	Infrastructure	Hugh Boyes, Prof Tim Watson	**https://petras-iot.org/project/positional-referencing-for-iot-at-the-edge-priote/**
Protecting your IoT products from purchase to disposal (Cyberhygiene)	University College London	Infrastructure	Dr John M. Blythe, Prof Susan Michie, Prof Jeremy Watson, Dr Carmen E. Lefevre	**https://petras-iot.org/publication/cyberhygiene-protecting-your-iot-products-from-purchase-to-disposal/**
Resilience and security in Low Power IoT (RSIOT)	University College London	Infrastructure	Dr M. Rio	**https://petras-iot.org/project/resilience-and-security-in-low-power-iot-rsiot/**
Resilient IoT on the Edge (RIoTE)	University of Warwick	Infrastructure	Prof Tim Watson, Dr Pedro Contreras, James McLachlan	**https://petras-iot.org/project/resilient-iot-on-the-edge-riote/**
Robustness-as-Traceability: Secure & Legal Calibration Workflows in IoT (Roast-IoT)	Strathclyde University	Infrastructure	Dr Shishir Nagaraja, Dr Angela Daly, Dr Mujeeb Ahmed, Dr Kaspar Ludvigsen	**https://petras-iot.org/project/robustness-as-traceability-secure-and-legal-calibration-workflows-in-iot-roast-iot/**
SDRIOTSS 2	University College London	Infrastructure	Dr Matt Ritchie, Dr Nial Peters, Colin Horne	**https://petras-iot.org/project/sdriotss-2/**
Securing IoT in Critical National Infrastructure – A PETRAS Demonstrator (SecCNIoT)	University of Bristol	Infrastructure	Prof Awais Rashid	**https://petras-iot.org/update/petras-demonstrators-bringing-research-into-the-real-world/**
Security and Performance in the IoT Smart Home (SPIoTSH)	University of Warwick	Infrastructure	Prof Carsten Maple	**https://petras-iot.org/project/security-and-performance-in-the-iot-smart-home-spiotsh/**
Security Risk Assessment of IoT Environments with Attack Graph Models (SECRIS)	Imperial College London	Infrastructure	Prof. E. Lupu, Dr Luis Muñoz-González	**https://petras-iot.org/project/security-risk-assessment-of-iot-environments-with-attack-graph-models-secris/**
Self-Sustained Blockchain-based Treasury System (BTS)	Lancaster University	Infrastructure	Dr Bingsheng Zhang	**https://petras-iot.org/project/self-sustained-blockchain-based-treasury-system-bts/**
Software Defined Receiver IoT Spectrum Survey SDRIOTSS (SDRIOTSS)	University College London	Infrastructure	Dr Matt Ritchie, Dr Nial Peters, Colin Horne	**https://petras-iot.org/project/software-defined-receiver-iot-spectrum-survey-sdriotss/**
Tangible Security (TanSec)	University of Nottingham	Infrastructure	Prof Derek Macauley, Dr Sameh Zakhary	**https://petras-iot.org/project/tangible-security-tansec/**
The Internet of Energy Things: supporting peer-to-peer energy trading and demand side management through blockchains. (P2P-IoET)	University College London	Infrastructure	Prof. D Shipworth	**https://petras-iot.org/project/the-internet-of-energy-things-p2p-ioet/**
The PETRAS Data Sharing Foundation: Building a Trustworthy Data Sharing Ecology for IoT Data Assets (PETRAS-DSF)	University of Southampton	Infrastructure	Dame Wendy Hall, Dr Laura Carmichael, Prof Michael Boniface	**https://petras-iot.org/project/the-petras-data-sharing-foundation-building-a-trustworthy-data-sharing-ecology-for-iot-data-assets-petras-dsf/**
The Red Teaming the Connected World (RETCON)	University of Oxford	Infrastructure	Dr Max Van Kleek, Prof Dave de Roure, Dr, Petar Radanliev, Dr Reuben Binns, Dr Alex Zugravu-Herciu	**https://petras-iot.org/project/red-teaming-the-connected-world-retcon/**

PETRAS Project Title	University	Sector	Project Team	URL
Trustworhty, Software-Defined Cyberattack Detection & Mitigation at the Network Edge (TruSDEd)	University of Glasgow	Infrastructure	Prof Dimitrios Pezaros, Prof Douglas J. Paul, Dr Kyle Simpson, Chris Williamson	**https://petras-iot.org/project/trustworthy-software-defined-cyberattack-detection-and-mitigation-at-the-network-edge-trusded/**
Uncanny AI (UnCanAI)	Lancaster University	Infrastructure	Prof Paul Coulton, Dr Joe Lindley, Fran Pilling, Dr Haider Ali Akmal	**https://petras-iot.org/project/uncanny-ai-uncanai/**
Understanding disruptive powers of IoT in the energy sector (Power2)	University of Bristol	Infrastructure	Prof Awais Rashid, Dr Ola Michalec	**https://petras-iot.org/project/understanding-disruptive-powers-of-iot-in-the-energy-sector-power2/**
PETRAS-IoT Data Management and Sharing Infrastructure: An Evolution of IoT Observatory (PEDASI)	University of Southampton	Infrastructure	Dame Wendy Hall	**https://petras-iot.org/update/petras-demonstrators-bringing-research-into-the-real-world/**
Securing IoT in Critical National Infrastructure – A PETRAS Demonstrator (SecCNIoT)	University of Bristol	Infrastructure	Prof Awais Rashid	**https://petras-iot.org/update/petras-demonstrators-bringing-research-into-the-real-world/**
Processes for Securing for Water Resource Management Systems (PSWaRMS)	University College London	Supply Chain and Control Systems	Prof Stephen Hailes, Dr Nilufer Tuptuk, Shreevanth Gopalakrishnan, Prof Tim Watson, Dr Pedro Contreras	**https://petras-iot.org/project/processes-for-securing-for-water-resource-management-systems-pswarms/**
Activities towards a PETRAS Buildings Management Information Demonstrator (EBIS+)	University College London	Supply Chain and Control Systems	Prof Peter T. Kirstein	**https://petras-iot.org/project/ebis-extending-bim-level-2-to-support-iot-security-demonstrator/**
Early Anomaly Detection for Securing IoT in Industrial Automation (ELLIOTT)	University College London	Supply Chain and Control Systems	Prof Stephen Hailes, Dr Nilufer Tuptuk, Shreevanth Gopalakrishnan	**https://petras-iot.org/project/early-anomaly-detection-for-securing-iot-in-industrial-automation-elliott/**
Economic Value of the Internet of Things in Cyberphysical Supply Chains (EVIoT)	University of Warwick	Supply Chain and Control Systems	Prof Carsten Maple; Dr Jonathan Cave; Prof Jim Smith; Prof Jan Godsell; Susan Wakenshaw, Rosario Micillo	**https://petras-iot.org/project/economic-value-of-iot-data-in-cyberphysical-supply-chains-eviot/**
Economies of Risk: Impact Assessment Model for the IoT (IAM)	University of Oxford	Supply Chain and Control Systems	Prof. Dave De Roure	**https://petras-iot.org/project/impact-assessment-model-for-the-iot-iam/**
From Logistics 4.0 to Digital Ports: A study in transformability using DLT's (DigiPort)	Imperial College London	Supply Chain and Control Systems	Prof Julie McCann, Dr Michael Breza	**https://petras-iot.org/project/digiport-from-logistics-4-0-to-digital-ports-a-study-in-transformability-using-dlts/**
Identifying Attack Vectors for Network Intrusion via IoT devices & Developing a Goal-Oriented Approach to Determining Impact Across Threat Surfaces (IoT Depends)	Cardiff University	Supply Chain and Control Systems	Prof Pete Burnapp	**https://petras-iot.org/project/identifying-attack-vectors-for-network-intrusion-to-determine-impact-across-threat-surfaces-iot-depends/**
Impact of Cyber Risk at the Edge: Cyber Risk Analytics and Artificial Intelligence CRatE)	University of Oxford	Supply Chain and Control Systems	Prof Dave de Roure, Dr Petar Radanliev	**https://petras-iot.org/project/impact-of-cyber-risk-at-the-edge-cyber-risk-analytics-and-artificial-intelligence-crate/**
Improving the Security of Centralised Trasnport Infrastructure Efficiency System (ISCTIES)	University College London	Supply Chain and Control Systems	Prof Jeremy Watson, Dr Uchenna Ani,	**https://petras-iot.org/project/improving-the-security-of-centralised-transport-infrastructure-efficiency-system-iscties/**
Integrity Checking at the Edge (ICE)	University of Cardiff	Supply Chain and Control Systems	Prof Pete Burnap, Dr Charith Perera, Dr Matthew Nunes, Dr Neetesh Saxena	**https://petras-iot.org/project/integrity-checking-at-the-edge-ice-for-operational-decision-support-ice-ods/**
Integrity Checking at the Edge for Operational Decision Support (ICE-ODS)	University of Cardiff	Supply Chain and Control Systems	Prof Pete Burnap, Dr Charith Perera, Dr Matthew Nunes, Dr Neetesh Saxena	**https://petras-iot.org/project/integrity-checking-at-the-edge-ice-for-operational-decision-support-ice-ods/**
Modelling for Socio-technical Security (MASS)	University College London	Supply Chain and Control Systems	Prof Jeremy Watson, Dr Uchenna Ani, Dr Mohammed Nasser Al-Mhiqani	**https://petras-iot.org/project/modelling-for-socio-technical-security-mass%e2%80%af/**
Newcastle Urban Sciences Building IoT (NUSBIoT)	University of Warwick	Supply Chain and Control Systems	Prof Carsten Maple, Dr John Mace, Hugh Boyes	**https://petras-iot.org/project/newcastle-urban-sciences-building-iot-nusbiot/**

PETRAS Project Title	University	Sector	Project Team	URL
Power Grid IoT System Protection and Resilience using Intelligen Edge (Power-SPRINT)	University of Warwick	Supply Chain and Control Systems	Dr Subhash Lakshminarayana, Prof Carsten Maple, Dr Hamidreza Jahangir	**https://petras-iot.org/project/power-grid-iot-system-protection-and-resilience-using-intelligent-edge-power-sprint/**
Secure Ontologies for IoT Systems (SOfIoTS)	University College London	Supply Chain and Control Systems	Prof Jeremy Watson, Dr Nilufer Tuptuk, Dr Aslam Jarwar, Jamie Tooth, Prof Michael Boniface	**https://petras-iot.org/project/secure-ontologies-for-iot-systems-sofiots/**
Securing High Value Goods using Self-Protecting Edge Compute (Logistics 4.0)	Imperial College London	Supply Chain and Control Systems	Prof Julie McCann, Dr Michael Breza, Dr Aisha Junejo	**https://petras-iot.org/project/logistics-4-0-securing-high-value-goods-using-self-protecting-edge-compute/**
Security Query-Based Systems (Sec-QBS)	Imperial College London	Supply Chain and Control Systems	Dr Yves-Alexandre de Montjoye, Bozhidar Stevanovski	**https://petras-iot.org/project/security-query-based-systems-sec-qbs/**
Adversarial Machine Learning on the Edge (AMLoE)	Imperial College London	Transport & Mobility	Prof Emil Lupo, Dr Luis Munoz-Gonzalez	**https://petras-iot.org/project/adversarial-machine-learning-on-the-edge-amloe/**
AI for Key Manamangement and Mitigating Attacks (AIKEMA)	University of Surrey	Transport & Mobility	Dr Haitham Cruickshank, Prof Klaus Moesner, Dr Waleed Hathal	**https://petras-iot.org/project/aikema/**
Blockchain Technology for IoT in Intelligent Transportation Systems (B-IoT)	Imperial College London	Transport & Mobility	Prof Michael Huth	**https://petras-iot.org/project/blockchain-technology-for-iot-in-intelligent-transportation-systems-b-iot/**
Cognitive & Socio-Technical Cybersecurity in Modern Railway System (CoSTCMoRS)	De Montfort University	Transport & Mobility	Dr Hongmei He, Prof Eerke Boiten,	**https://petras-iot.org/project/cognitive-and-socio-technical-cybersecurity-in-modern-railway-system-costcmors/**
Designing Dynamic Insurance Policies Using IoT (DDIP-IoT)	Imperial College London	Transport & Mobility	Prof. M. Huth	**https://petras-iot.org/project/designing-dynamic-insurance-policies-using-iot-ddip-iot/**
Increasing User Trust in Mobility-as-a-Service IoT ecoSystem (UMIS)	University of Southampton	Transport & Mobility	Dr Richard Gomer, Dr Gary Wills, Dr Temitope Omitola, Dr Niko Tsakalakis	**https://petras-iot.org/project/increasing-user-trust-in-mobility-as-a-service-iot-ecosystem-umis/**
IoT for Transport and Mobility Demonstrator (IoT-TraM)	University of Warwick	Transport & Mobility	Prof Carsten Maple	**https://petras-iot.org/update/iot-tram-enabling-more-secure-and-private-connected-and-autonomous-vehicles/**
Lightweight Security and Privacy for Geographic Personal Data and Location Based Services (GEOSEC)	University of Surrrey	Transport & Mobility	Dr Haitham Cruickshank, Dr Philip Asuquo, Dr Ao Lei	**https://petras-iot.org/project/lightweight-security-and-privacy-for-geographic-personal-data-and-location-based-services-geosec/**
Multimodal AI-based Security at the Edge (MAISE)	University of Glasgow	Transport & Mobility	Dr Jose Cano Reyes, Dr Jeremy Singer, Dr Sye Loong Keoh, Idris Zakariyya	**https://petras-iot.org/project/multimodal-ai-based-security-at-the-edge-maise/**
Multi-Perspective Design of IoT Cybersecurity in Ground and Aerial Vehicles (MAGIC)	University of Glasgow	Transport & Mobility	Dr Michele Sevegnani, Prof Muffy Calder, Dr Meng Wei Xu	**https://petras-iot.org/project/multi-perspective-design-of-iot-cybersecurity-in-ground-and-aerial-vehicles/**
Privacy in Connected Autonomous Cars and Smart Transport Systems (P-CARS)	University of Surrey, University of Warwick	Transport & Mobility	Dr Jia Liu, Prof Mehrdad Dianati, Prof Carsten Maple	**https://petras-iot.org/project/privacy-and-trust-in-connected-autonomous-cars-and-smart-transport-peiesi/**
Smart Road & Street Maintenance, Pricing and Planning (RoadMaPP)	Lancaster University, Imperial College London	Transport & Mobility	Prof Nigel Davies, Dr Mike Harding, Prof John Polak, Dr Thomas Heinis	**https://petras-iot.org/project/roadmapp/**
Trade-off Management between Safety and Cybersecurity (TOMSAC)	Coventry University	Transport & Mobility	Dr Giedre Sabaliauskaite, Dr Jeremy Bryans, Prof Siraj Ahmed Shaikh	**https://petras-iot.org/project/trade-off-management-between-safety-and-cybersecurity-tomsac/**
Transport and Mobility Demonstrator Audit (TMDA)	University of Warwick	Transport & Mobility	Prof Carsten Maple	**https://petras-iot.org/project/transport-and-mobility-demonstrator-audit-tmda/**
IoT for Transport and Mobility Demonstrator (IoT-TraM)	University of Warwick	Transport & Mobility	Prof Carsten Maple	**https://petras-iot.org/update/iot-tram-enabling-more-secure-and-private-connected-and-autonomous-vehicles/**

PETRAS CENTRE TEAM, 2023

Eleri Jones – Head of PETRAS Centre Team, **Halil Uzuner** – Research Programme Manager, **Sarah Hardy** – Senior Marketing and Communications Manager, **Katerina Papakyriakopoulou** – Marketing and Communications Officer, **Peter Novitsky** – Synthesis Fellow, **Oktay Cetinkaya** – Synthesis Fellow, **Gideon Ogunniye** – Synthesis Fellow, **Joe Bourne** – Synthesis Fellow, **Ruth Dollard** – Operations Manager, **Rob Ebsworth** – Operations Manager**, Emilie Didier** – Business Development Executive, **Rajab Said** – Business Partnership Executive, **Claire Coulton** – Lead for Monitoring and Cohort Development, **Amaya Hana** – Project Liaison Lead, **Loraine Daly** – PA to PETRAS Director

We would like to thank everyone who has been a member of the PETRAS Centre Team between 2019-2023, including all of the Masters of Public Administration (MPA) candidates from STEaPP (UCL), who joined us as PETRAS Associates each year, bringing much needed energy and insight to our work.

In Memory of Sam King

1.7.1972 – 11.2.2023

In February 2023, PETRAS was sad to announce the death of our Research Programme Coordinator, Sam King.

Sam was with PETRAS from the very beginning and was not only a central and intrinsic member of the team but was also a great and brilliant friend to many. It is difficult to convey how much she will be missed.