RESEARCH INSTITUTE
IN TRUSTWORTHY INDUSTRIAL CONTROL SYSTEMS

IDENTIFYING, COMMUNICATING & SOLVING CYBER THREATS TO UK NATIONAL INFRASTRUCTURE

RITICS IS FUNDED BY

National Cyber Security Centre
a part of GCHQ

EPSRC
Pioneering research and skills

CYBER THREATS TO INDUSTRIAL CONTROL SYSTEMS

INDUSTRIAL CONTROL SYSTEMS (ICS) ARE COMPUTERS THAT MONITOR AND MANAGE INDUSTRIAL TASKS. THEY ARE FOUND IN MULTINATIONALS, SMES AND NATIONAL INFRASTRUCTURE, FROM RAIL NETWORKS TO POWER PLANTS.

ICS have evolved from self-contained and isolated networks to being heavily interconnected with IT systems and other networks and services. This has led to new cybersecurity vulnerabilities and the potential for inter-organisational, inter-industry and international threats. This emerging type of risk was highlighted by the Stuxnet attack on an Iranian nuclear facility, and the more recent attacks on a German Steel Mill and the Ukrainian power grid.

RITICS

CO-FOUNDED BY PROF CHRIS HANKIN - THE CURRENT RITICS DIRECTOR - AND DR DEEPH CHANA IN 2014, RITICS IS A RESEARCH PROGRAMME OF FIVE ACADEMICALLY LED AND INDUSTRIALLY LINKED CYBERSECURITY PROJECTS DISTRIBUTED AMONGST FIVE UK UNIVERSITIES.

RITICS is one of the UK's 3 national cybersecurity institutes and was established to address three key research questions:

// **DO WE UNDERSTAND THE HARM THAT THREATS POSE TO ICS AND BUSINESS?**

// **CAN WE CONFIDENTLY ARTICULATE THESE THREATS AS BUSINESS RISK?**

// **ARE THERE NOVEL EFFECTIVE AND EFFICIENT INTERVENTIONS?**

"RITICS HAS ESTABLISHED THE UK AS A FRONT RUNNER IN CYBERSECURITY RESEARCH RELATING TO INDUSTRIAL CONTROL SYSTEMS AND THE GOVERNANCE AROUND THEM. THE SIGNIFICANT INDUSTRY INTEREST AND SUPPORT FOR MANY OF THE PROJECTS HIGHLIGHTS THE IMPORTANCE OF THE TOPICS AND THEIR APPLICABILITY TO REAL WORLD ISSUES WHICH NEED URGENT ATTENTION"

UK NATIONAL CYBER SECURITY CENTRE (NCSC)

IMPACT

5. **RESEARCH** PROJECTS

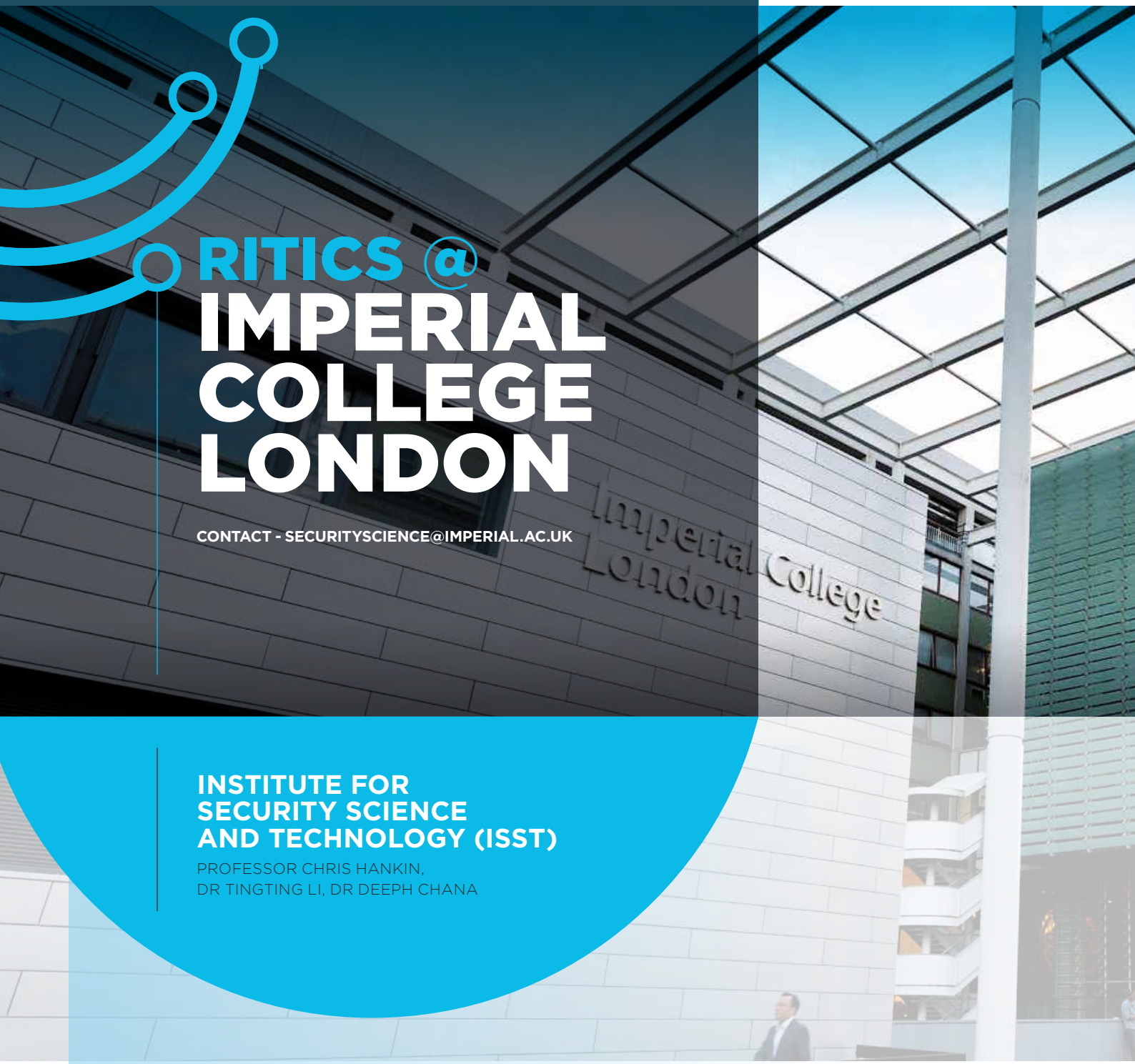
8. **FURTHER ACADEMIC** COLLABORATORS, INCLUDING 1 MOU SIGNED

16. **INDUSTRY** PARTNERS

35. **RESEARCH** PUBLICATIONS

83. **ENGAGEMENT** EVENTS INTERNATIONALLY

40+ **£MILLION FUNDING** LEVERAGED



RITICS @ IMPERIAL COLLEGE LONDON

CONTACT - SECURITYSCIENCE@IMPERIAL.AC.UK

INSTITUTE FOR SECURITY SCIENCE AND TECHNOLOGY (ISST)

PROFESSOR CHRIS HANKIN,
DR TINGTING LI, DR DEEPH CHANA

RITICS @IMPERIAL HAS PRODUCED COST-EFFECTIVE MODELS AND TOOLS FOR PROTECTING INDUSTRIAL CONTROL SYSTEMS FROM CYBER THREATS. THESE HELP ANALYSE VULNERABILITIES, OPTIMISE DEFENCE STRATEGIES AND DETECT NETWORK INTRUSIONS.

FOR MORE INFORMATION VISIT **WWW.RITICS.ORG/RITICS**

INDUSTRY PARTNERS | ATKINS | Symantec. | GENERAL DYNAMICS

Imperial College London

INTRODUCTION

Industrial Control Systems (ICS) are computers that monitor and manage industrial tasks. They are found in multinationals, SMEs and national infrastructure, from rail networks to power plants. They have evolved from self-contained and isolated networks to being heavily interconnected with IT systems and other wider networks and services. This has led to new cybersecurity vulnerabilities and the potential for inter-organisational, inter-industry and international threats.

Developing solutions first requires an understanding of where the vulnerabilities are, how attackers might exploit them and what the economic consequences of threats are.

OUR MAIN SUCCESSES

// ANALYSIS OF VULNERABILITIES

We generated all possible paths for an Advanced Persistent Threat attack (e.g. Stuxnet) in an example ICS network using Answer Set Programming, and quantified the risk of each using Bayesian Networks.

We modelled the optimal decisions of attackers (e.g. attack method and delivery system depends on time and defences) targeting ICS users to inform defence policy.

The security and safety of a system can impact each other, complicating analysis. We developed a framework to understand the relationship between security and safety in ICS and the impact of a given security policy, e.g. how a security policy makes a system more secure but less safe.

// DEFENCE STRATEGIES

We showed optimal defence strategies can be computed by using Particle Swarm Optimisation simulations of the interplay between attackers and defenders.

We showed Software diversity – a method to de-risk the presence of zero-day exploits (unknown cybersecurity vulnerabilities) - can be optimised through strategic deployment of products using their comparative known vulnerabilities.

// INTRUSION DETECTION

We created an ICS network intrusion detector that outperformed current state-of-the-art techniques. Our system uses deep learning to anticipate normal network traffic, and alerts if there are deviations from this.

FUTURE CHALLENGES

The accelerating development of Industry 4.0 over the next five years will amplify existing threats. Critical Manufacturing has already become the top sector reporting incidents to The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and the increasing use of mobile devices to remotely monitor and interact with Industry 4.0 systems will only increase attack opportunities.

In this context, the original challenges posed to RITICS remain valid. Based on our insights and new interactions with industrial partners we will deepen our understanding of, and develop proposals for, achieving secure-by-default, which is at the heart of the UK's national cybersecurity strategy.

SCEPTICS

SYSTEMATIC EVALUATION PROCESS FOR THREATS TO INDUSTRIAL CONTROL SYSTEMS

CONTACT - J.M.EASTON@BHAM.AC.UK

UNIVERSITY OF BIRMINGHAM

PROFESSOR CLIVE ROBERTS,
DR TOM CHOTHIA,
DR JOHN EASTON

SCEPTICS HAS DEVELOPED A SET OF COMMON PROCESSES FOR THE RAIL INDUSTRY TO IDENTIFY CYBERSECURITY VULNERABILITIES IN THEIR INDUSTRIAL CONTROL SYSTEMS, AND PRIORITISE THEM FOR INVESTIGATION USING MORE DETAILED THREAT ANALYSIS TOOLS.

FOR MORE INFORMATION VISIT **WWW.RITICS.ORG/SCEPTICS**

INDUSTRY PARTNERS | nationalgrid | TRL Technology one step ahead | RSSB

UNIVERSITY OF BIRMINGHAM

INTRODUCTION

Bespoke Information and Communications Technology (ICT) systems in the rail industry have gradually been replaced by Commercial Off The Shelf (COTS) solutions due to commercial and operational pressures.

COTS solutions risk increasing the attractiveness of the railways to cyberattackers due to shared vulnerabilities, attack mechanisms and exploits targeted in other sectors.

Rail industry chiefs worldwide recognise that the risk of cyberattack is increasing, but many are unsure of how to begin building an understanding of the extent of the problem, or the steps required to address it.

OUR MAIN SUCCESSES

We have shown how at both the system and sub-system levels security analysis tools developed in other domains can be applied within the context of the rail industry.

In particular, we have shown how the dependencies between shared ICT systems across the industry create a web of activity that is impossible to fully understand without detailed mathematical analysis. We have also shown how probabilistic modelling techniques may be applied to industry data to gain new system-level insights into this issue.

At the sub-system level, we have been applying known analysis techniques from other domains to specific railway hardware and processes, with activity including an analysis of the MAC algorithm used in the Euroradio security layer, and the creation of proposals around a new process for key management within ERTMS.

FUTURE CHALLENGES

One of the biggest challenges we faced was the low level of maturity and awareness of security issues within the industry. In the early stages of the project, responsibility for cybersecurity rested with individual stakeholder companies, if it was considered at all. This made it difficult to gain a system-level understanding of key processes and platforms.

During the life of the project, railways have been moving to address this problem. Clear lines of responsibility have also been created for cross-industry steering in the cybersecurity domain (via the Rail Delivery Group). Also, many of the key stakeholders have been developing new processes to manage cyber issues, and raising awareness amongst their respective workforces and boards. Following work on SCEPTICS, a number of industry stakeholders have expressed interest in taking the work forwards. The proposals around key management for ETCS have been particularly well received, with contacts from companies including RSSB and SNC Lavelin keen to pursue the topic further.

CAPRICA

CONVERGED APPROACH TOWARDS RESILIENT INDUSTRIAL CONTROL SYSTEMS AND CYBER ASSURANCE

CONTACT
DAVID.LAVERTY@QUB.AC.UK OR J.HASTINGS@QUB.AC.UK

CENTRE FOR SECURE INFORMATION TECHNOLOGIES (CSIT) / ENERGY, POWER AND INTELLIGENT CONTROL (EPIC)

PROFESSOR SAKIR SEZER,
DR DAVID LAVERTY, DR KIERAN MCLAUGHLIN

CAPRICA HAS PRODUCED SECURE, RELIABLE AND RESILIENT SYNCHROPHASOR TECHNOLOGIES THAT ENABLE NEXT-GENERATION SMART GRID CONTROL STRATEGIES. THESE FAR EXCEED INDUSTRY-STANDARD APPROACHES IN ACCURACY AND DEPENDABILITY OF PHYSICAL MEASUREMENTS, AND SECURITY OF SYNCHROPHASOR COMMUNICATIONS.

FOR MORE INFORMATION VISIT **WWW.RITICS.ORG/CAPRICA**

INDUSTRY PARTNERS

sse EMC² Statnett

Queen's University Belfast

INTRODUCTION

The smart grid is an evolution of the electric grid with efficiency and resilience improved by modern information technologies. The integration of renewable and distributed energy sources, and the emergence of prosumers who both consume and generate electricity, means the electrical grid increasingly behaves as a cyber-physical system. Vulnerabilities in cyber components can directly affect the underlying physical grid.

Phasor Measurement Units (PMUs) are a key enabling technology for smart grids as they can accurately record grid conditions for operational data. CAPRICA investigates how state-of-the-art PMU technologies can be advanced, and used for secure future smart grid applications.

OUR MAIN **SUCCESSES**

// PHYSICAL TEST-BED DEMONSTRATION

We developed a physical test-bed using an innovative "synchronous island" control strategy. A synchronous island can occur when a grid section becomes disconnected, e.g. due to an electrical fault. This is increasingly important as embedded electricity generation increases. Using custom PMU devices and a process to maintain synchronicity, we demonstrated in the lab the first ever synchronous island supported by an IEC 61850-90-5 communications infrastructure.

// PMU DEVICES FOR ASSURED SYNCHROPHASOR MEASUREMENT

We developed a modular PMU device design concept, allowing the incremental improvement of domains such as phasor estimation and secure communication, and the rapid prototyping and verification of new components prior to platform integration. Responding to industry concerns, we developed methodology to assess the compliance of several PMU devices against recognised standards, and identify the trustworthy metrics for each device. We developed several components that represent a sophisticated reference implementation for secure and high-quality phasor measurements.

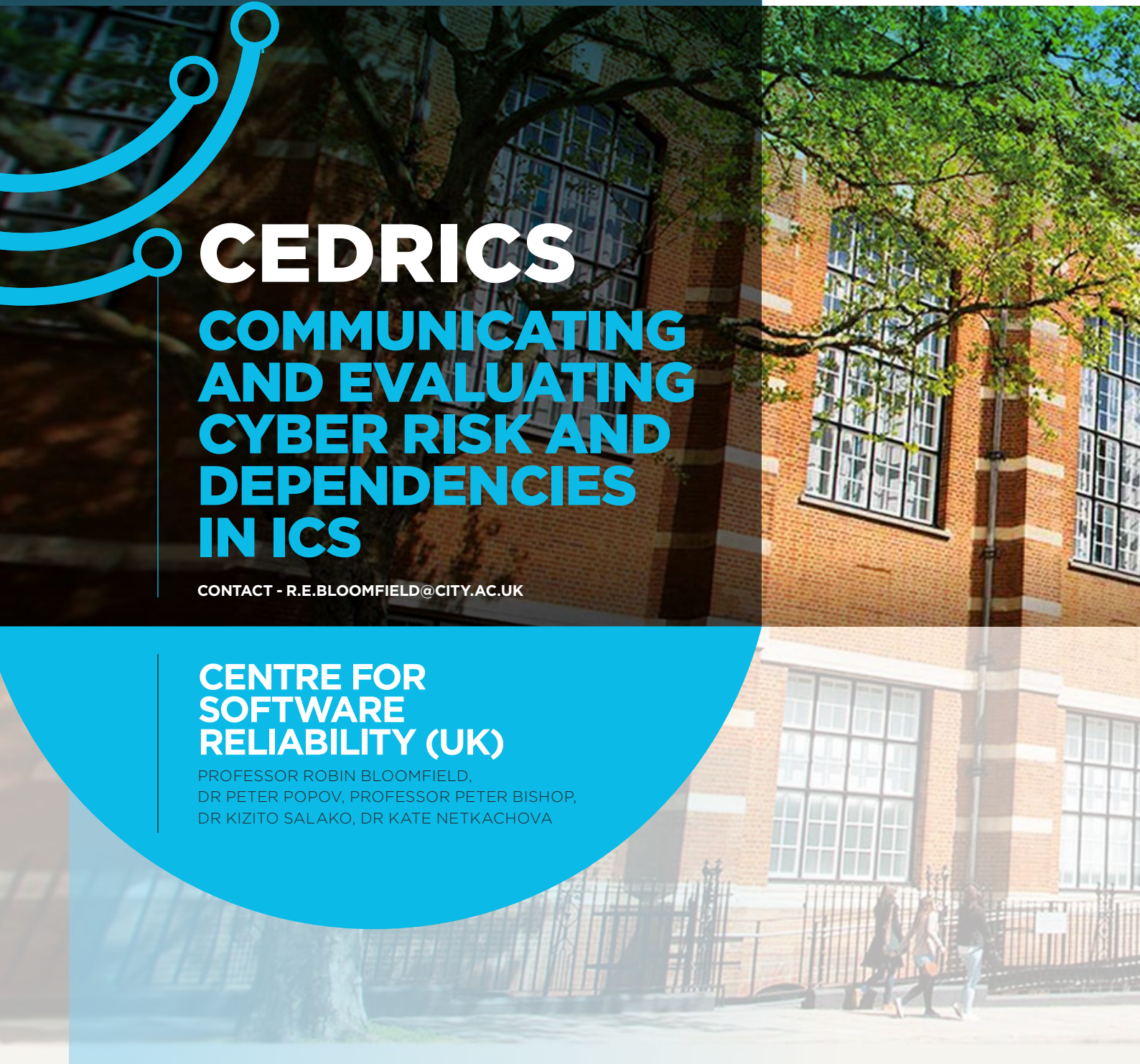
// SECURE AND RESILIENT COMMUNICATIONS

We produced the first published research implementing a security solution compatible with the relevant IEC synchrophasor communciations standard. We also developed a secure IEC proxy to protect legacy devices using the more common IEEE standard, and an intrusion detection approach to monitor insecure substation communications where legacy devices remain.

FUTURE **CHALLENGES**

The solutions we developed raise further cybersecurity challenges, e.g. the questionable dependability of GPS for synchrophasor calculations. We believe this can be addressed by new off-the-shelf atomic clock technologies promising high quality assurance of data.

With electric system, PMU, and IDS models already developed to understand control of the studied synchronous system, we can investigate how closely PMUs can interoperate with IDS technologies for automated response to detected intrusions. A truly converged security approach where PMUs and IDS technologies merge presents an exciting opportunity for further exploration.



CEDRICS

COMMUNICATING AND EVALUATING CYBER RISK AND DEPENDENCIES IN ICS

CONTACT - R.E.BLOOMFIELD@CITY.AC.UK

CENTRE FOR SOFTWARE RELIABILITY (UK)

PROFESSOR ROBIN BLOOMFIELD,
DR PETER POPOV, PROFESSOR PETER BISHOP,
DR KIZITO SALAKO, DR KATE NETKACHOVA

CEDRICS HAS DEVELOPED SCALABLE APPROACHES TO COMMUNICATING THE CYBERSECURITY COMPONENT OF BUSINESS RISK TO STAKEHOLDERS, AND A RISK-BASED APPROACH TO ASSESSING DEFENCE-IN-DEPTH OF INDUSTRIAL CONTROL SYSTEMS.

FOR MORE INFORMATION VISIT **WWW.RITICS.ORG/CEDRICS**

INDUSTRY PARTNERS

PSYMETRIX AN ALSTOM COMPANY · ALSTOM · pwc

CITY UNIVERSITY LONDON

INTRODUCTION

For resource-limited organisations to deploy cybersecurity interventions the threats, vulnerabilities, their business impact and mitigations need to be articulated and understood. CEDRICS explored how stakeholders at different levels can obtain the understanding they need of cyber risks.

Articulating business risk due to cyberthreats requires an understanding of the complex relationship between threats, control and measurement systems, and the physical assets. A Claims, Arguments and Evidence (CAE) framework can be used to enable reasoning and communication about these risks especially when supported with detailed models of systems and adversary behaviour.

OUR MAIN **SUCCESSES**

//METHODOLOGY FOR STRUCTURED SECURITY-INFORMED CASES

We developed a claims, arguments and evidence (CAE) framework for creating rigorous, structured argumentation for complex engineering systems with cybersecurity explicitly addressed.

Our approach enhances the existing assurance-case methodology. It increases the depth and range of analysis, addresses the trustworthiness of the evidence and assessment process, facilitates challenge, and helps to communicate cyber risks to different stakeholders.

// ANALYSIS OF INTERDEPENDENCIES AND DEFENCE IN DEPTH

We have developed an approach to assessing defence-in-depth of industrial control systems with specific focus on cyber-security. This involves an analysis of interdependencies in critical infrastructures and both probabilistic and deterministic modelling of the effects of the cyberattacks (e.g. the loss of power in power system), and also attacks on special purpose software used to support the decisions taken by operators in control centres.

We produced scenarios to analyse known attacks and the effectiveness of layered defences, and abstract models of an Adversary for future attacks exploiting unknown (zero-day) vulnerabilities.

// APPLICATION TO INDUSTRIAL CASE STUDIES

Working with industrial partners we applied our work in different domains, including:

- Creating a security-informed safety case for a Security Gateway in avionics.
- Developing an approach to demonstrate security-informed safety of a smart device in a nuclear application.
- Evaluating security and reliability of a power transmission system.
- Supporting the development of policy and assessing the impact of security issues on safety regulation.

FUTURE **CHALLENGES**

An increased connectivity and autonomy of road and rail vehicles, and modernisation of the existing infrastructures such as the digital railway, will present significant challenges and will require efficient approaches especially to security-informed safety.

Based on our insights and new interactions with industrial partners, we expect to develop approaches with increased emphasis on automated reasoning. In addition, attacks on special purpose decision supporting software (e.g. operators in the control centres) is one emerging threat area that requires further research and where our work will be applicable.

MUMBA
MULTI-FACETED METRICS FOR ICS BUSINESS RISK ANALYSIS

CONTACT - MARASH@COMP.LANCS.AC.UK

SECURITY LANCASTER INSTITUTE

PROFESSOR AWAIS RASHID (PI),
DR KAROLINA FOLLIS, DR JEREMY BUSBY,
DR ALBERTO ZANUTTO, DR. SYLVAIN FREY,
BEN SHREEVE

MUMBA DEVELOPED UNDERSTANDING OF THE GAP BETWEEN MANAGERIAL EXPECTATIONS AND THE ACTIVITIES OF CYBERSECURITY OPERATIVES, AN ANALYSIS OF ICS CYBERSECURITY DECISION MAKING, AND A FRAMEWORK TO DERIVE BUSINESS-FOCUSED CYBERSECURITY METRICS.

FOR MORE INFORMATION VISIT **WWW.RITICS.ORG/MUMBA**

INDUSTRY PARTNERS | ATKINS | AIRBUS | Raytheon | THALES

Lancaster University

INTRODUCTION

Cybersecurity risk is not just a technical construct and is often impacted by social and organisational factors. Current metrics for risk decision-making in ICS cybersecurity are technical, ordinal and mostly unrelated to factors used in business risk analysis.

Articulating cyber risk as business risk requires multi-faceted metrics that are principally driven by business risk concepts, and considered both along and across various facets of an ICS setting, such as the ICS itself, enterprise systems, business processes, people, 3rd parties and new technologies and practices.

OUR MAIN **SUCCESSES**

// EXPOSING THE GREY AREA IN ICS SECURITY

Our fieldwork revealed that ICS security is a grey area shaped by competing demands of various stakeholders, e.g. managers, control engineers and enterprise IT personnel. Security workers must respond to unexpected situations arising from the technologies in use, the supply chain and employees across the organisation. We showed that ICS security and resilience can be improved if the knowledge from security workers is acted upon. This will need the mission of all employees to be redefined to promote collective responsibility for cybersecurity.

// BUSINESS-FOCUSED SECURITY METRICS

We developed a methodology that promotes the integration of business goals, organisational context and security risks into the security metrics development process. It builds on the goal-question-metrics approach and provides security-specific templates and methodological elements. This enables the alignment of security metrics with a business perspective, and requires more than just a technical perspective on the problems at hand.

// TABLETOP GAME OF ICS CYBER SECURITY DECISION-MAKING

We have developed a tabletop game to study the decision-making behaviours of various ICS stakeholders (e.g., managers, security experts, engineers), and allow them to experiment with threats, learn about decision making and its consequences, and reflect on their own perception of risk.

Players must manage the cybersecurity of a Lego® ICS infrastructure, considering a number of potential threats, known infrastructure-vulnerabilities, past and ongoing cyberattacks and budget limitations. So far 30 games have been played with over 150 players of varying security expertise, mostly from industry. Data analysis has identified characteristic decision-making patterns: some good, with balanced priorities, open-mindedness and adapting strategies based on inputs that challenge one's pre-conceptions; some bad, with excessive focus on particular issues, confidence in charismatic leaders; and some ugly, with "tunnel vision" syndrome by over-confident players.

FUTURE **CHALLENGES**

The MUMBA framework and the game will be extended to tackle the challenges of assessing cybersecurity risk in ICS supply chains.

RITICS IS COORDINATED BY THE INSTITUTE FOR SECURITY SCIENCE AND TECHNOLOGY, IMPERIAL COLLEGE LONDON.

THE INSTITUTE FOR SECURITY SCIENCE AND TECHNOLOGY WAS FOUNDED IN 2008 AS ONE OF IMPERIAL COLLEGE LONDON'S GLOBAL CHALLENGE INSTITUTES.

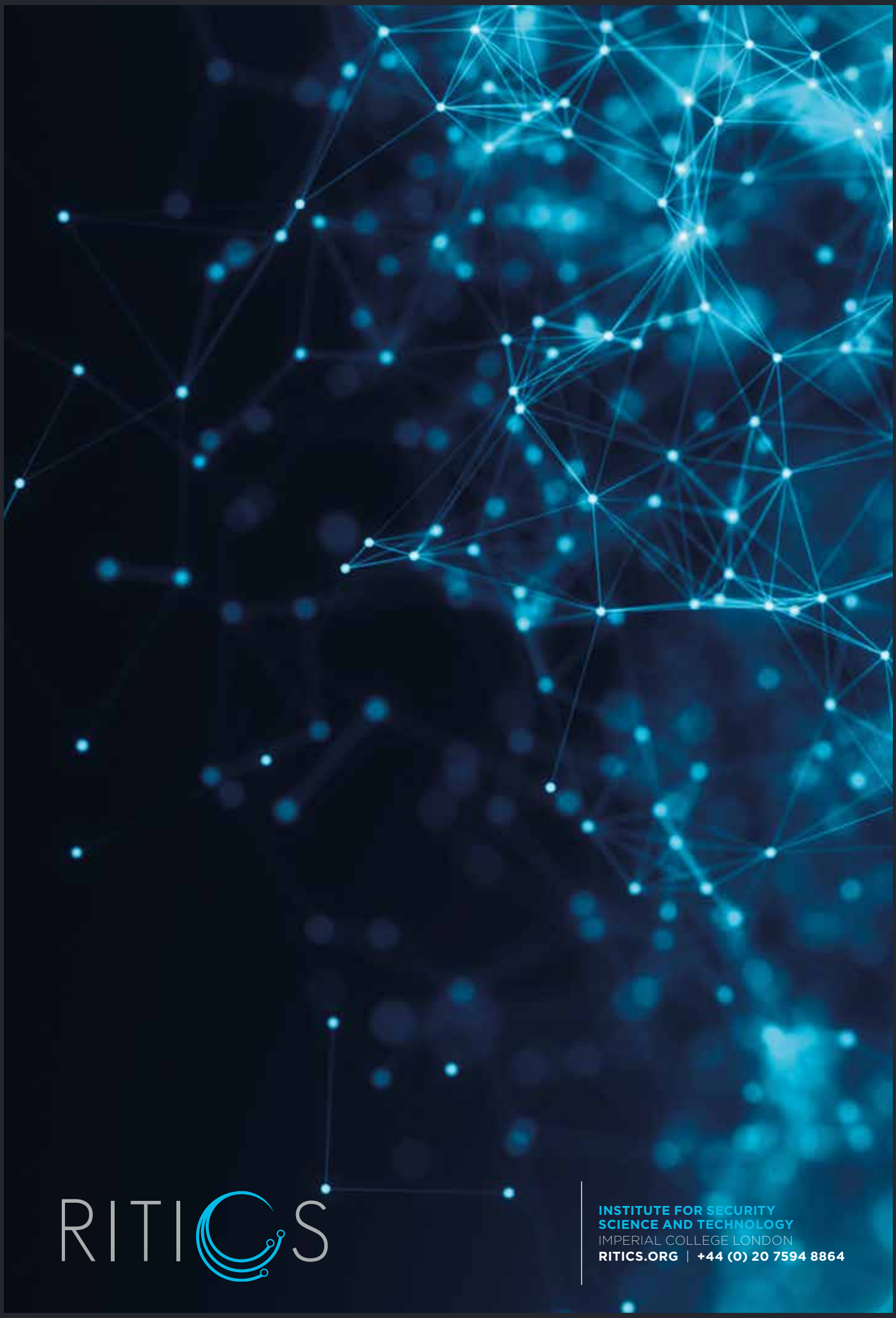
These were set up to promote interdisciplinary working to meet the greatest challenges faced by society. The Institutes each serve as focal points for multidisciplinary activities and interfaces to external stakeholders, as well as formulating and applying new areas of knowledge, technological solutions and scientific advice.

Geo-political uncertainties, climate change and changing cyber and physical attack methods give rise to a constantly evolving security landscape. At the ISST we envisage, design and coordinate the application of science and technology to answer the grand security challenges raised.

We seek to improve security and resilience across a range of scales, from protecting the individual to ensuring the security of whole populations. Our core research themes include Cybersecurity, Cyber-Physical Systems Security, Physical Security, Financial Systems Security, Healthcare Security, and Climate and Environmental Security.

IMPERIAL.AC.UK/SECURITY-INSTITUTE
@IMPERIAL_ISST


RITICS



INSTITUTE FOR SECURITY SCIENCE AND TECHNOLOGY
IMPERIAL COLLEGE LONDON
RITICS.ORG | **+44 (0) 20 7594 8864**