Imperial College London

INSTITUTE FOR SECURITY SCIENCE AND TECHNOLOGY

RITICS

Research Institute in Trustworthy Inter-connected Cyber-physical Systems

A portal to cutting edge UK research into the cyber security of cyber physical, critical systems

RITICS is a network of academics, industrialists and government working on cyber security in industry.

It is coordinated by the Institute for Security Science and Technology; Imperial College London's hub for security research and engagement.

FUNDED BY:

National Cyber Security Centre
a part of GCHQ

UKRI Engineering and Physical Sciences Research Council

COORDINATED BY:

Imperial College London

INSTITUTE FOR SECURITY SCIENCE AND TECHNOLOGY

Contents

Letter from RITICS Director, Chris Hankin

Welcome to the 2023 RITICS Brochure, the third in our series. We will provide annual updates during this next phase of the Research Institute for Trustworthy Inter-connected Cyber-physical Systems.

Founded in 2014, RITICS emerged as a consortium comprising five research projects funded by the Engineering and Physical Sciences Research Council (EPSRC) in collaboration with the Centre for Protection of National Infrastructure (CPNI). Initially focused on industrial control systems, our emphasis was on understanding the physical risks posed by cyber interference, communicating these risks, and devising innovative mitigations. The projects delved into specific sectors like power distribution (CAPRICA), the digital railway (SCEPTICS) and general modelling techniques (CEDRICS and RITICS@IC). Risk was addressed by CEDRICS and MUMBA. Notably, the Birmingham SCEPTICS team played a pivotal role in establishing the UK Rail Research and Innovation Network (UKRRIN). Concurrently, we fostered strong ties with industries and facilitated the growth of the Industrial Control Systems Community of Interest (ICS CoI) into a substantial network. Our contributions extended to shaping cyber security strategies, such as the Rail Cyber Security Strategy, and engaging in European standards development through ERNCIP.

The second phase of RITICS (2018–2022) marked a shift in funding, with the National Cyber Security Centre (NCSC) taking over support for research activities, while EPSRC continued backing the Director. RITICS remained actively involved with the Community of Interest, contributing to cyber security strategies across sectors. This brochure focuses on the key developments during this period, detailing projects supported in this phase. With the enforcement of the Network and Information Security Directive (NIS) in mid-2018, RITICS-funded projects explored its implications on essential service operators. Other initiatives were driven by community needs and NCSC priorities. In 2022, a new funding scheme initiated two short-term fellowships, further detailed in this brochure.

The current phase of RITICS started in January 2023. The Director role is now supported by NCSC and UKRI will support a research programme. The first call for research projects took place at the end of 2022 and, as we go to press, we are awaiting the announcement of the successful proposals. The Director role includes funding for the continuation of the fellowship scheme and we are currently appointing two fellows, one is concentrating on economic aspects of cyber security for critical infrastructure and the other is focused on digital twins and modelling. We will report more on these in the next edition of this brochure.

I hope that you find the following pages interesting and informative. Our contact details are in the About Us section; RITICS is an open community and if you would like to receive regular updates and news about our events, please get in touch.

Letter from ISST Co-Director, Deeph Chana

Problems related to resilience, security and insecurity can no longer be considered in silos of geography or discipline. Events in any one part of the world can have direct consequences on the most distant locations, often in unexpected ways, whilst security concerns in one aspect of society or industrial sector can rapidly lead to impact or contagion risk to others. Commercial activities and motivations and state-on-state conflict, for example, are increasingly difficult to decouple into separate concerns. A few years ago, this interconnected, complex, description of the security landscape may have been regarded as a theoretical construct related to the future, bearing little resemblance to our present reality. However, events such as the COVID-19 pandemic, climate-driven food insecurity in regions like East Africa, the withdrawal of NATO troops from Afghanistan and the Russian-Ukraine war have highlighted the very real and present relevance of approaching security research with a model of complexity in mind.

At the ISST we recognize that the development of science, technology and innovation is inextricably linked to problems of security, defence and resilience across all societies and cultures. The mycelial nature of digital technologies and the proliferation of computing has ushered in a new state of human existence which has profoundly altered the way we establish connections, communicate, analyse information, make decisions, collaborate, view ourselves, view each other and vie for power over finite resources. Geopolitical discourse is now driven by social media platforms and their associated algorithms, computing systems collaborate with human beings to operate our critical infrastructure systems in a complex cyber network and the emergence of blockchain technologies is driving revolutions in finance, the meaning of identity, the structure of businesses and the fundamental characteristics of nations and economies. These component trends are collectively manifest in a hyper-complex cyber-physical world where the risks of conventional threats are amplified by novel means – e.g. the risk of nuclear conflict can be increased through mass disinformation – and where, simultaneously, a raft of new vulnerabilities and security issues are emergent. This trend is set to continue as we stand on the threshold of a wave of global transformations driven by a set of profound emerging and disruptive technologies, including machine learning, web 3.0, additive manufacturing, biological and synthetic materials engineering, and the proliferation of human activity in space

Whether through education, research or innovation, understanding how to analyse this security landscape, prioritise aspects within it and design the next generation of mitigations and resilient systems is the mission of our Institute.

About Us

Research Institute in Trustworthy Inter-connected Cyber-physical Systems (RITICS) is a portal to cutting-edge UK research into the cyber security of cyber-physical, critical systems.

About critical infrastructure systems

Critical infrastructure systems are those that provide critical services, such as transport, energy, water and telecommunications. Underpinning services, such as high-value manufacturing, are also considered critical systems. These critical infrastructure systems can be described as being cyber-physical, in that they contain networked computers which can control physical parameters. This opens them up to cyber security threats, which can have physical consequences.

Background

The programme is funded by the Engineering and Physical Sciences Research Council (EPSRC) and the National Cyber Security Centre (NCSC).

RITICS was founded in 2014 as a cyber security institute set up by the UK Government in conjunction with EPRSC. Its early focus was to improve cyber security of Industrial Control Systems. RITICS was renewed and relaunched in spring 2018 as one of six cyber security institutes, with funding for a further five years, now sponsored by the NCSC in partnership with EPSRC.

RITICS is an open community of academic researchers. Anyone who is conducting relevant work is encouraged to join the community. Members contribute to and receive a regular newsletter, are invited to RITICS meetings and gain access to a large community of like-minded researchers.

The first two calls of the second phase of RITICS took place in Summer and Autumn 2018, and have given rise to the first research projects of the second phase. This booklet summarises the initial work being done in these projects.

For more information

Discover the latest research and funding news, copies of the RITICS newsletter, and contact details for the whole RITICS network at: **www.ritics.org**

To learn more about the RITICS community or Council, please contact us at: **ritics@imperial.ac.uk**

Projects

AIR4ICS: Agile Incident Response for Industrial Control Systems

De Montfort University

Agile Incident Response for Industrial Control Systems (AIR4ICS) is a new Incident Response framework that improves situational awareness and information sharing to reduce the time to successful identification, mitigation and remediation. Through the use of agile tools and methodologies incident responders are able to work effectively to identify and assign tasks to transition from reactive to proactive defence, with incident responders empowered to take ownership of their tasks and to develop their cross-functional skillsets.

Attacks against Industrial Control Systems (ICS) have risen year on year since the introduction of what is arguably the first targeted cyber-physical attack, Stuxnet. Incident response within ICS and the Operational Technology estate is even more complex than traditional IT incident response. Cyber incident response within Industrial Control Systems (ICS) is characterised by high levels of uncertainty and unpredictability, requiring a multi-disciplined team that encompasses personnel business operations, Operational Technology (OT), IT, security operations and media engagement to be effective. Such teams require a dynamic decision framework to allow ICS operators to maintain services during the recovery of full operating capability. Rigid, procedural incident response processes are increasing the predictability of the defence efforts and make it more difficult to protect the remaining infrastructure and business functions in the context of fast-pivoting and multi-pronged cyber attacks. Especially when IR crosses IT/OT boundaries, communication between stakeholders, often from different disciplines and organisational hierarchies, is frequently impeded and situational awareness is decreased. Agile approaches on the other hand welcome changing requirements and are driven by value and the understanding of the system by a cross-functional team that can manage conflicting stakeholder requirements. This approach is therefore geared to environments where change is constant and the environment and objectives are not clearly identified or defined. AIR4ICS advocates the integration and evaluation of agile methods and practices, used in e.g. SCRUM and KANBAN, to provide a security incident response team with the ability to respond quickly to changes whilst maintaining the focus on the business and its value-chains.

To understand the issues faced by those tasked with defending ICS interviews were conducted with professionals across industry and government. Thematic analysis was then used to identify consistent challenges impacting the efficiency of the response effort. These challenges formed the requirements for the new framework to address.

Analysis of the different agile methodologies identified tools and techniques from multiple approaches that could be adapted and provide benefits for the incident response environment. Using scrum as the basis for a series of time-boxed sprints for cadence teams are able to ingest feedback, information and changing requirements with a minimal delay allowing resources to be deployed more efficiently and effectively based upon the current situation. Tools such as

the Incident Backlog and Risk Poker have been developed to allow team members to better prioritise tasks and ensure that all aspects of the investigation retain momentum.

A key aspect of protecting ICS is a cross-functional team, however given the often-transient nature of teams investigating incidents can be difficult for managers to have an accurate understanding of what skill exist within their teams. To combat this a template for capability maps have been developed, these multi-dimensional graphs factor in aspects such as area, value, risk and performance gap to present an easy-to-understand representation of the current team capabilities. These graphs can be used to quickly identify areas of strength and critical areas where additional capability is required.

The framework was refined through three cyber defence exercises, with both the Red and Blue teams comprising professionals from industry. The exercises utilised the research Security Operations Centre and CYRAN Cyber Range at DMU to provide an immersive sandbox environment in which to assess the techniques in a realistic environment. Each exercise focussed on different elements of Critical National Infrastructure: a port, a pharmaceutical plant and a water treatment facility. The hybrid capability of CYRAN facilitated the inclusion of physical equipment, both DMU's own test beds and equipment provided by Airbus and Rolls Royce, to increase the value of the exercises for both participants and the research as a whole. Findings from each exercise were analysed and the feedback used to further refine the proposed framework. As a result the framework has been designed to be fully modular, allowing teams to pick and choose those elements best suited to current operational procedures with a minimum of disruption. As the maturity of the agile integration within the team progresses more aspects can be included to further realise the benefits to the team.

AIR4ICS ensures that relevant information is available in a clear and concise manner, providing resources and techniques to attribute and present information to all stakeholders. By ensuring that all team members have a greater understanding of the overall response strategy they are better able to make informed decisions in their own work.

Architecting Multi-Actor Cybersecurity

University of Glasgow

Cybersecurity entails a sharing of risk that requires a collective effort to mitigate. A collaborative effort among relevant stakeholders can contribute to understanding the latest threat landscape and commit to reducing vulnerabilities and minimising the impact of incidents. Cyber maturity assessments, that focus on the area of control of an individual company, rest on a relatively narrow evidence base without considering dependencies across extended supply chains. This research is looking at different approaches to building cybersecurity capability across interdependent organisations, considering operational perspectives and the wider engineering solution that cybersecurity needs to be deployed and managed within.

The aim is to utilise Enterprise Systems Engineering (ESE) methods to map resilience and preparation beyond organisational boundaries, and to guide contributions from multiple owners to a mutual cybersecurity. The need for an increasingly distributed situation awareness will be explored through application of ESE to cybersecurity capability development across critical infrastructures.

Systems engineering addresses complex technical systems that involve many stakeholders, ESE is an adaptation of the systems engineering concept to socio-technical environments by including a significant human and organisational aspect. Systems engineering specifies components of functionality using a whole system approach. ESE engineers the interactions between components of a system to enable an expanded set of capabilities. ESE prioritises the interconnectedness and dependencies because the design extends across organisations to achieve the required capability, while acknowledging the limits to cooperation where the interests of different actors are more disparate. Considering the implications of cybersecurity for organisational dynamics, the differences in human and technical aspects of a design are explored, such as interconnection of human capability through IT and OT cross-functional teams, alongside the technical necessity to segment traffic between systems.

Patterns of interaction with Operational Technologies have been changing in recent times with more remote working. In addition, their exposure to supply chain challenges includes a reliance on vendor support and how this is managed across various types of ownership and different responsible areas. This research is designing an Enterprise Systems Engineering (ESE) framework applicable to supply chain challenges considering cybersecurity as a core functional requirement. This framework intends to facilitate cybersecurity improvements across a network of organisations by integrating the contribution of multiple actors to reduce risks and proposing accountability structures. The use of resilience measures is also being investigated as a tool to improve operational resilience across diverse actors with clearer responsibilities for assurance and whole system resilience.

This research also considers the inter-organisational cooperation implied by regulatory efforts with Network and Information Security (NIS) and the opportunity & ability to meet cyber regulatory responsibilities, by looking at how regulatory oversight and operator behaviours are influencing the preparation and response to cybersecurity for critical infrastructure. In particular, the broadening and deepening application of the NIS Directive and how this might aid the area of supply chain challenges. This aims to inform improvements and focus further support where needed the most.

The framework proposed during this research could also be usefully applied to other socio-technical enterprises undergoing change.

Cloud-enabled Operation, Security Monitoring, and Forensics (COSMIC)

Queen's University Belfast

The COSMIC project (Cloud-enabled Operation, Security Monitoring, and Forensics) at Queen's University Belfast addresses security and resilience challenges in the modernisation of legacy industrial control system infrastructure. Many current industrial systems were designed long before the vision of industry 4.0, and often lack basic security features. The presence of legacy devices presents security and interoperability challenges, and operational resilience requirements that are a barrier to adopting emerging technology platforms, such as cloud. COSMIC addresses technical solutions towards integrating legacy devices with cloud-based platforms that can support supervisory and control type operations, while providing monitoring and oversight, with consideration for security and resilience capabilities.

The project has developed a bump-in-the-wire cloud connectivity device and a cloud platform, and demonstrates low-latency secure operation of two cyber-physical test cases via the cloud, 1) a PLC testbed controlling a robot arm, and 2) a smart grid use-case focusing on phasor measurement unit (PMU) communications that support real-time control and monitoring of substations. This leverages our previous research in OpenPMU (openpmu.org). Secure gateway platforms are developed to support low-latency encryption and transmission of insecure legacy communication protocols (e.g. IEEE C37.118.2). The developed cloud platform supports data-collection and log-parsing of operational data, presented and accessible via the cloud through the COSMIC analytics and visualisation platform. As a key resilience component, in the event of failure in a cloud application or connectivity issues at the cloud, mechanisms have been developed to support secure failover, ensuring that multiple cloud instances are available in different geographic locations capable of maintaining seamless operations between the cloud platform and the industrial systems.

Developing Pedagogy to Optimise Forensic Training in Safety-Related Industrial Control Systems (ICS)

University of Glasgow

Pedagogy deals with the theory and practice of teaching and how these influence student learning. Research in computing science has begun to develop an evidence base to guide the teaching of key concepts, see for example the Royal Society report on computing education 'After the Reboot'. First steps have also been taken to develop the pedagogy of cyber security. A recent RISCS workshop stressed the role that the GCHQ Research Institutes must play in influencing best practice in pedagogy. However, most existing guidance focuses on schools and Universities. There is little or no empirical work on effective approaches for training professional systems engineers. We will address this omission. The aim of this proposal is to develop an evidence base

and then to derive principles that provide industry and government with effective training in forensic engineering, focussing on safety-critical ICS applications.

Diversity by Design

Cardiff University

Diversity-based approaches have been studied as an effective strategy to enhance the security and resilience of complex systems. The property of diversity was originally used in biology to indicate the sustainability and survivability of an ecosystem. Inspired by this, diversity-based approaches have been studied since the 1970s as an effective strategy to enhance the security and resilience of complex systems. The underlying idea is diversifying the system components to make the overall system highly resistant against sudden changes, faults and attacks. It is a more concerning issue in digital systems as an identified vulnerability could quickly spread over all digitally identical components and give rise to catastrophic damage. Optimal diversification can effectively avoid replicated attacks and increase the attacking difficulty of the adversary.

Nevertheless, most works on diversity-based security to date have not used any metrics to quantify system diversity. Even though some work proposed diversity metrics in software diversity specifically, there is still an urgent need for a generic approach to assess and quantify diversity, which can be applied in a variety of interconnected networks and systems. Most diversification strategies suffer from high deployment costs, and thus accurately measuring diversity would be crucial to evaluate the effectiveness of those diversification plans prior to the actual deployment.

This project aims to quantify the system diversity by identifying similarly vulnerable structures of components in interconnected systems. It mainly uses Graph Neural Networks (GNN) and other machine learning techniques to convert network graph data into vector representation and search for similarly vulnerable structures. We can then effectively evaluate human-input diversification strategies prior to actual deployment. The proposed work also provides an effective way to represent the CNI and other interconnected systems with the focus of identifying similarly vulnerable points of a system, which can provide insights into the resilience of the dependencies against replicated attacks and avoiding cascading failure.

Effective Solutions for the NIS Directive – Supply Chain Requirements for Third Party Devices

University of Birmingham

This project developed a methodology and framework that enables ICS operators, asset owners and the wider supply chain to quickly and effectively verify the security of third party devices, from diverse supply chains. The shift from the traditional bespoke systems and components used in critical national infrastructure towards commercial-off-the-shelf systems of systems means that the

compromise of one device can affect the security of an otherwise well-designed system.

These Operational Technology (OT) devices are fundamentally different from the traditional IT, where different requirements are placed on these systems, and, as a result, these devices can be hard to assure from a practitioner, supply chain and end asset-owner viewpoint. This project assessed and developed ways that the assurance of such devices can be undertaken to aid in the compliance of the NIS Directive, providing detailed guidance to asset owners for procurement, and assessing these devices prior and post-deployment. This project has developed a body of knowledge of the ICS threat landscape, identifying the key and prominent risks to Industrial Control Systems, categorising them into detectable ways, and, using open source threat intelligence, the window of exposure for such vulnerabilities.

The project carried out a critical analysis of existing tools for IT and OT cyber security assurance, identifying the most effective analysis methods from easy to use (e.g. automated solutions), through to those for use by experts (e.g. reverse engineering) for use across a wealth of ICS devices and systems.

How Many Shades of NIS? Understanding Organisational Cybersecurity Cultures and Sectoral Differences

University of Bristol

The project will develop an empirically-grounded understanding of the role and impact of organizational cybersecurity culture and practice across essential infrastructure sectors on the UK's implementation of the NIS directive. Through fieldwork and subsequent analysis of the data and modelling of cybersecurity controls in the extensive Bristol Cyber Security testbed, we will uncover organizational and sectoral differences, for instance, in the way which people work, what technologies (software/hardware) are relied upon, what additional compliance requirements exist. This will yield key insights about the NIS objectives that are already achieved, the ones difficult to effectively realize and potential blind spots arising from organizational cultures and sectoral practices. This will lead to an understanding of the drivers and potential obstructions to UK's implementation of NIS across operators of essential infrastructures. To achieve this, the project brings together an inter-disciplinary team at the University of Bristol drawing upon expertise in socio-technical approaches to cybersecurity of critical national infrastructure (Rashid), human and organizational aspects of security (van der Linden) and Milyaeva.

Interconnected Safe and Secure Systems (IS3)

City, University of London

Interconnected systems: Define a generic reference model of a "resilient organisation" as a socio-technical entity operating a cyber-physical system (CPS) dependent on other CPS operated by their respective operators. Explore the role of higher fidelity models as a way of ranking the alternative ways of implementing a given reference model and research if credible simplified models are suitable for interdependency and dependency analysis. Explore issues of scale and composition by applying the generic infrastructure model in a multi infrastructure system.

Safety and security: Develop an understanding of the problems and priorities of industry in security-informed and safety issues and an understanding of how decisions are made at the moment that involve trade-offs and the combination of objective and subjective judgements. Continue to develop the justification framework based on Claims, Arguments, Evidence which integrates objective and subjective evidence and explicitly combines informal reasoning with formal model-supported deduction. Research model-based techniques to analyse systematically the trade-offs and dependencies that are often complex technically, organisationally and institutional.

NDN for Secure Industrial IoT Networking

Queen's University Belfast

In the past decade, the insecurity of industrial control systems (ICS) and smart grid network protocols such as IEC 60870, IEC 61850, Modbus, DNP3, etc., became a significant focus for systems operators, suppliers, and researchers. Many potential cyber vulnerabilities and risks to physical infrastructure have been identified in the research community. In more recent years these have played a role in real-world attacks, for example the CrashOverride malware is observed to have been able to interact with several ICS protocols (www.cisa.gov/uscert/ncas/alerts/TA17-163A).

Many protocols associated with ICS evolved from serial links by adopting TCP/IP encapsulation, for instance IEC 60870-5, which is a standard for power system monitoring and control associated with utilities such as electric power systems or water treatment. This protocol, like many others, is heavily based on data objects. For example, IEC 60870-5-101 uses Application Service Data Unit (ASDU) addresses, where data is classified into information objects, each provided with a specific logical address. Arguably, this data model lends itself more naturally to a data-oriented communication approach, rather than the host-oriented TCP/IP approach, whereby data must be encapsulated within multiple layers for transmission. This often requires various middleware and gateways to translate and repackage data, or to provide layers of security. For example, the operation of Phasor Measurement Units (PMUs) in smart grids typically relies on a hierarchy

of Phasor Data Concentrator (PDC) middleboxes.

In this project we therefore consider two technology paradigms, the first is the Industrial Internet of Things (IIoT), which is a rapidly developing area that addresses the proliferation of highly interconnected and ubiquitous embedded devices in ICS. The second technology we consider is Named Data Networking (NDN), which is an approach to develop networking infrastructure that is data-centric rather than host-centric (based on connecting hosts end-to-end). Significantly for our research, NDN has security features 'baked in' at the network layer, offering potential advantages for IIoT.

Communication in NDN is driven by data consumers, through the exchange of two types of packets: Interest and Data. Both packet types carry a name that identifies a piece of data. All data available to the network is named and identified using hierarchical structured names, which may be local or global. For example, 'QUB/ICS/historian/20210303' could be the name used for some data logged on 3 March 2021. Data can be broken down into chunks, such as '…20210303/1', '…20210303/2', and so on. For a consumer to indicate interest in specific data, i.e. it wants a copy of this data, the consumer sends an Interest packet to the network with the name of the desired data. Routers use this name to forward the Interest toward the data producer(s). This basic exchange is illustrated in Fig. 1.

With NDN, security is built into the data itself. The intention is to secure the content, not the container or communication channel. The security actions are performed directly at the network layer with content identification provided in data names. Each piece of data is signed together with its name, securely binding them. Data signatures are mandatory. Integrity protection guarantees the authenticity of the data bound to the name by including the producer signature of the data plus its name. Confidentiality (via data encryption) is optional, and applications can distribute data encryption keys as encrypted NDN data, limiting the data security perimeter to the context of a single application. This is an exciting concept with potential to be genuinely transformative, allowing developers to focus on data access at an application level, with security mechanisms for integrity and confidentiality handled by the network layer, agnostically and transparently.

PMUs are a key enabling technology of Smart Grids. They provide time synchronised measurements which allow system operators unprecedented visibility of electricity networks. Queen's University Belfast has expertise and experience investigating cyber security issues related to PMU smart grid environments, having previously completed RITICS projects CAPRICA, investigating security implementations of the IEC 61850-90-5 protocol, and COSMIC, investigating secure migration of SCADA control platforms to the cloud. These projects had a significant impact in the ongoing OpenPMU project (http://www.openpmu.org) which in turn led to the spin-out Phasora Ltd.

PMUs enable novel real-time operational control methodologies which facilitate integration of low carbon technologies, including renewable generation, electric vehicles, heat pumps, which are considered vital to meeting international

obligations related to climate change. NDN features address many of the shortfalls of current communication technology for distributed renewable energy generation. For example, IEEE and NASPI working groups have recently identified the challenges of telecoms complexity and cyber security concerns as barriers to the widespread deployment of PMU applications. One of the key weaknesses is the reliance on PDCs, requiring unpacking, refactoring and repackaging of PMU data many times in the communication path. NDN offers an opportunity to reduce this overhead and provide security features lacking in present systems.

Consequently, this project addresses these problems and investigates applying NDN to IIoT. Using PMU communications as a practical case-study, we will particularly focus on NDN's proposed approaches to security and evaluate its suitability for low-resource embedded PMU devices. We aim to consider how do our findings apply to broader IIoT contexts, considering cyber security advantages and disadvantages, performance constraints, and barriers to adoption by industry.

The NIS Directive and Supply Chain Resilience

University of Glasgow

Evaluating the impact of NIS implementations on Supply Chain Resilience of critical infrastructures

This project investigated the experience of implementing the NIS Directive from the different perspectives of competent authorities, operators, and suppliers. The effectiveness and impact of responsibilities assigned by the Cyber Assessment Framework (CAF) were analysed across the Water, Energy, and Transport sectors. The extent to which improvements in supply chain cybersecurity were being achieved through NIS implementations were evaluated.

The NIS Directive is acting as a tool for change by introducing new roles and responsibilities in cybersecurity, with a focus on maintaining essential services to society. The NIS principles and objectives provide a set of contributing outcomes and a profile per sector is guiding the achievements of NIS. The expectation of a deep understanding of extensive supply chains and an oversight of supply chain risks has presented a challenge to operators of essential services. Furthermore, procurement practices have been assuring the cybersecurity of supplier companies rather than assuring the product or service being used within a customer context. In some cases, the adoption of common approaches, in cooperation and trusted partnerships, has been able to progress further with cybersecurity improvements than individual organisations working in isolation. In essence, the project

emphasised supplier relationships as a strategic asset and striking a balance between control and cooperation, such as utilising formal controls of contractual arrangements alongside collaborative commitments to integrate skills and processes.

The project recommended some enhancements to Supply Chain guidance including:

- Emphasis on risk reduction and reducing the impact of incidents.
- Common security requirements per sector.
- Combined supplier assurance process to reduce overhead on OES and suppliers.
- Cyber exercises involving suppliers.
- Utilising points of governance in the supply chain, where controls or cooperation are required with important suppliers.
- Regular review of commitments to maintain accountability between operators and suppliers.

Impact

The project provided engagement with industry and policymakers, offering feedback to public-private partnerships, and influencing policy enhancements. This included the following contributions:

- Forum Europe panel debate with ENISA on 'Coherent and Consistent Cyber Security'
- Presentation to European industry events including Smart Grid Forums and EUTC.
- Presentations on building capability in supply chains to UK OES, CAs and NCSC.
- Academic review of supplier assurance activities.
- Input to UK and EU NIS Reviews.

Imperial College London

INSTITUTE FOR SECURITY SCIENCE AND TECHNOLOGY

RITICS
Imperial College London
Level 2 Admin Office, Central Library
South Kensington Campus
London SW7 2AZ

E-mail: ritics@imperial.ac.uk

ritics.org