Issue 02/2025

RITICS Newsletter

FELLOWSHIP AWARDEES 2025

We are delighted to welcome our 2025 RITICS Fellows, whose pioneering research will address some of the most pressing challenges in cyber-physical system (CPS) security. Each fellow brings a unique perspective and expertise to the RITICS community, and their work will contribute to advancing our collective understanding of how to secure critical infrastructure in an increasingly connected world.

Below, we provide a brief overview of their research aims and areas of focus.

Confidence in Cyber-Physical System Security: *Taimoor Khan, Greenwich University*

This fellowship explores the foundational question: *"How do we have confidence in the security of a cyber-physical system (CPS)?"* The research focuses on key sub-areas including security assurance, testing, operational technology (OT) interface security, and security risk management, as framed in the NCSC Cyber Physical Problem Book.
The project aims to build a conceptual framework and taxonomy to support future interdisciplinary research in CPS security. It will examine how different scientific communities—spanning security testing, risk management, policy,

and regulation—approach the challenge of establishing and evaluating security confidence in CPS.

A central goal is to investigate and compare **model-driven** and **data-driven** approaches used to generate evidence for assessing how well a system meets its security objectives. This includes understanding how confidence in CPS security is formed at both design-time and run-time in response to cyber and non-cyber threats, vulnerabilities, and cascading risks.

The research will address five key questions:

1. What are the different notions of "confidence" in CPS security as supported by current assurance, testing, OT, and risk management practices?
2. What are the fundamental requirements for establishing each of these notions?
3. How is confidence measured—through qualitative, quantitative, or hybrid approaches?
4. What are the inherent strengths and limitations of each approach?
5. How can these varied notions be unified into a cohesive framework for quantifying security confidence?

Ultimately, this work will contribute to clearer definitions, more robust metrics, and practical tools for evaluating the security posture of cyber-physical systems across a variety of domains.

UK Strengthens Cyber-Physical Infrastructure Security Amid Rising Threats, *Pantelis Koutroumpis, Oxford University*

Cyber-Physical Systems (CPS), integral to daily life and national infrastructure, are facing escalating cyber threats due to increasing interconnectivity. The UK is now the third most targeted country for cyber-attacks globally, behind the US and Ukraine, according to the House of Commons (2023). In response, the head of the National Cyber Security Centre recently warned that UK providers of essential services must take these threats seriously.

Over the past decade, academic researchers and regulators have ramped up efforts to address vulnerabilities in Critical National Infrastructures (CNI) while multiple studies have shown that organised groups pose the single greatest threat to Industrial Control Systems (ICS). In an effort to identify threat actors and their methods, researchers have focused on predicting the implications of cascading system failures by modelling attack paths and performing in-depth penetration testing.

On the regulatory front, the UK government is actively planning to further deter these threats by implementing the **Cyber Security and Resilience (CSR) Bill** in 2025. This legislation follows extensive overhauls of the existing NIS directive (akin to NIS2 in the EU) and is expected to broaden regulatory coverage, increase penalties, and raise compliance demands. Acknowledging the targeted equipment cyber-attacks, the **Product Security and Telecommunications Infrastructure (PSTI) regulation** introduced in 2023 aims to cover all smart products sold in the UK, imposing strict security requirements and penalties for non-compliance.

These regulatory interventions jointly form a two-pronged strategy— a holistic top-down enforcement via the **Cyber**

Security and Resilience Bill and increasing bottom-up requirements via the **Product Security and Telecommunications Infrastructure regulation**. Together, they aim to shift the cost burden of cyber-attacks from society to organisations, incentivising stronger security practices and reallocating the negative externalities from improper security practices to their rightful owners. This fellowship will address whether these changes are sufficient and proportional to the risks posed by the threat actors, given the concerns around increases in the cost-of-service provision that could potentially strain labour and capital resources, especially in non-market sector.

FUNDING OPPORTUNITIES

We are excited to announce the availability of a small fund to support members of the RITICS community. This funding can be utilised for various purposes such as travel grants, workshop organisation, feasibility studies, and similar activities. Individual awards will be capped at £5,000.

To apply, please submit a one-page document (A4 size) with reasonable margins and a minimum font size of 11pt. The application should outline the purpose of the funding, the benefits it will bring to the RITICS community, and include a detailed breakdown of the costs.

Applications will be reviewed twice a year, during Spring and Autumn. Preference will be given to early career researchers. All applications to be sent to ritics@imperial.ac.uk

UPCOMING EVENTS

Register and save the dates for the following events:

Title	Location	Date	Registration
RITICS Fest	London Venue: TBC	2nd to 3rd September 2025	Register here

GET IN TOUCH

Email us with your news that you would like to share with the community or reach out on LinkedIn