NATIONAL CYBER-PHYSICAL INFRASTRUCTURE ECOSYSTEM

Department for Science, Innovation & Technology

Opening Address from the Department of Science, Innovation and Technology

NCPI WORKSHOPS

Security and Resilience

Proudly Supported by:

CATAPULT Digital

CATAPULT Connected Places

CATAPULT High Value Manufacturing

WORKSHOP OUTLINE

Security and Resilience

Security and resilience are not just necessities, they are critical enablers for unlocking the true potential of the systems within systems.

By collaborating across sectors and staying informed about emerging threats, we can collectively build a safer and more resilient cyber-physical ecosystem.

This workshop covered one of the Department for Science, Innovation and Technology (DSIT) identified enablers for an effective national cyber-physical infrastructure ecosystem. Its aim was to explore and understand the current landscape, explore gaps and what potential actions are needed for the future landscape.

The workshop brought together over 50 stakeholders to explore security and resilience challenges and solutions and develop consensus around priority recommendations within this space.

Roundtable sessions

The session was opened by an esteemed panel covering perspectives from Government, Industry and Academic. Prof Jeremy Watson, UCL, Director of the PETRAS National Centre of Excellence for IoT Systems security, Hugh Boyes, leading industry expert on cyber threats in the built environment and infrastructure protection, Dr Alison Vincent, technical thought leader and NED for Connected Places Catapult and Dr Andrew F2, research lead within the NCSC's cyber physical team.

This set the ground for two roundtable sessions exploring key themes with attendees as detailed on the right.

NCPI Workshop on Security & Resilience

Hosted at Digital Catapult, London

Agenda

13:00 Welcome

13:05 Panel discussion (as referenced under roundtable sessions)

13:45 Roundtable - Session 1 – Understanding risks and threats

15:00 Break

15:10 Roundtable - Session 2 – Building secure systems

16:30 Wrap up and next steps

WORKSHOP OUTPUT

Delivery of recommendations

Collective effort across NCPI stakeholders to identify recommendations

Roundtable findings were recorded digitally by a nominated person at each table, and findings across the day sorted and prioritised between each session of discussion.

Each table was asked to provide additional information on post-it notes with comments from their discussions and a nominated individual was asked to feedback to the the whole room at the end of the day.

We started discussions around understanding risks and threats to obtain perspectives from those in the room. Following this segment, participants then looked at what makes a secure system and how one can be built, sharing insights from their own domains.

This method enabled a clear presentation of views, insights and considerations and top recommendations for Government.

As referenced on the right-hand side, security and resilience can act an enabler of the benefits of innovation and significance for the broader ecosystem and wider national cyber physical infrastructure programme areas.

Security and Resilience as an enabler of the benefits of innovation and the significance for the broader ecosystem and wider NCPI

Holistic Protection: Integrated risk management across domains allowing seamless integrated safeguards into complex and interconnected systems without impacting productivity.

Resilient Infrastructure: Redundancy, adaptive capability to cyber threats and preparedness.

Policy and Regulation: Standards, public safety, GDPR, NIS Directive.

Technological Innovation: Advanced solutions with new technology innovation, continuous improvement.

Global Cooperation: International standards, collaboration - five eyes sharing evolving risks to critical infrastructure.

ROUNDTABLE VIEW

"Security must be integrated from the beginning to build trust and resilience across all business practices."

RESILIENCE

"Cybersecurity should be as fundamental in education as health and safety, ensuring future professionals are prepared."

EDUCATION

"Policy-based access control is essential to regulate and secure access to critical systems and data."

CRITICAL SYSTEMS

”Proactive habits like promotes a culture of vigilance and continuous security improvement."

CYBER HABITS

"Meeting insurer requirements can drive adherence to cybersecurity best practices across industries."

BEST PRACTICES

"Structured ontologies and taxonomies improve our understanding of cyber-physical infrastucture, enhancing threat detection."

ONTOLOGIES & TAXONOMIES

ROUNDTABLE INSIGHTS

"Understanding sector-specific risks is crucial to making cybersecurity a proactive business priority."

UNDERSTANDING RISKS

”Cybersecurity training in schools and workplaces is key to building a secure digital future."

EDUCATION

"Regularly updating access controls and training staff are vital to adapting to evolving security threats."

ACCESS CONTROL

"Integrating cyber habits into daily routines creates a shared priority for organisational security."

CYBER HABITS

"Aligning security measures with insurance criteria helps reduce risk and improve coverage eligibility."

INSURABILITY

"AI-driven analysis of structured data helps predict threats and automate effective responses."

DATA MODELS

CONSIDERATIONS

Key thoughts captured from participants

Participants identified several key considerations for strengthening cyber-physical infrastructure (CPI), starting with the need to bridge **educational gaps** in cybersecurity. Traditional technical degrees often lack comprehensive cybersecurity components, leaving graduates ill-prepared to address the complexities of interconnected systems. This approach should align with "**secure by design**" principles, embedding security considerations at every stage of development.

Consistency in cybersecurity standards across sectors was another significant theme, underscoring the importance of a uniform regulatory approach. Cybersecurity regulations can be fragmented, leading to uneven security practices across industries. Participants highlighted the value of **industry and academic partnerships** to foster open information sharing and develop collaborative solutions. Creating case studies and conducting scenario planning within these partnerships can further enhance resilience by enabling sectors to learn from one another's experiences and avoid siloed security approaches.

Research and development (R&D) emerged as a critical priority, particularly the need for cross-technology innovation to address emerging threats. Rather than focusing on isolated technologies, R&D should promote solutions that **span multiple sectors**, recognising the interconnected nature of CPI systems. Scenario planning were identified as valuable tools in this context, allowing organisations to anticipate potential cascading failures before they occur.

Public engagement and resilience were also focal points, with strong support for campaigns to **raise awareness** of CPI threats and cybersecurity best practices. In addition to raising awareness, participants emphasised the importance of regular resilience testing, moving beyond sector-specific simulations to broader, multi-sector exercises. There is an opportunity to conduct comprehensive scenario planning that tests response strategies for potential cascading failures. These efforts can provide a deeper understanding of vulnerabilities and help develop robust defences to ensure the continuity and security of critical systems.

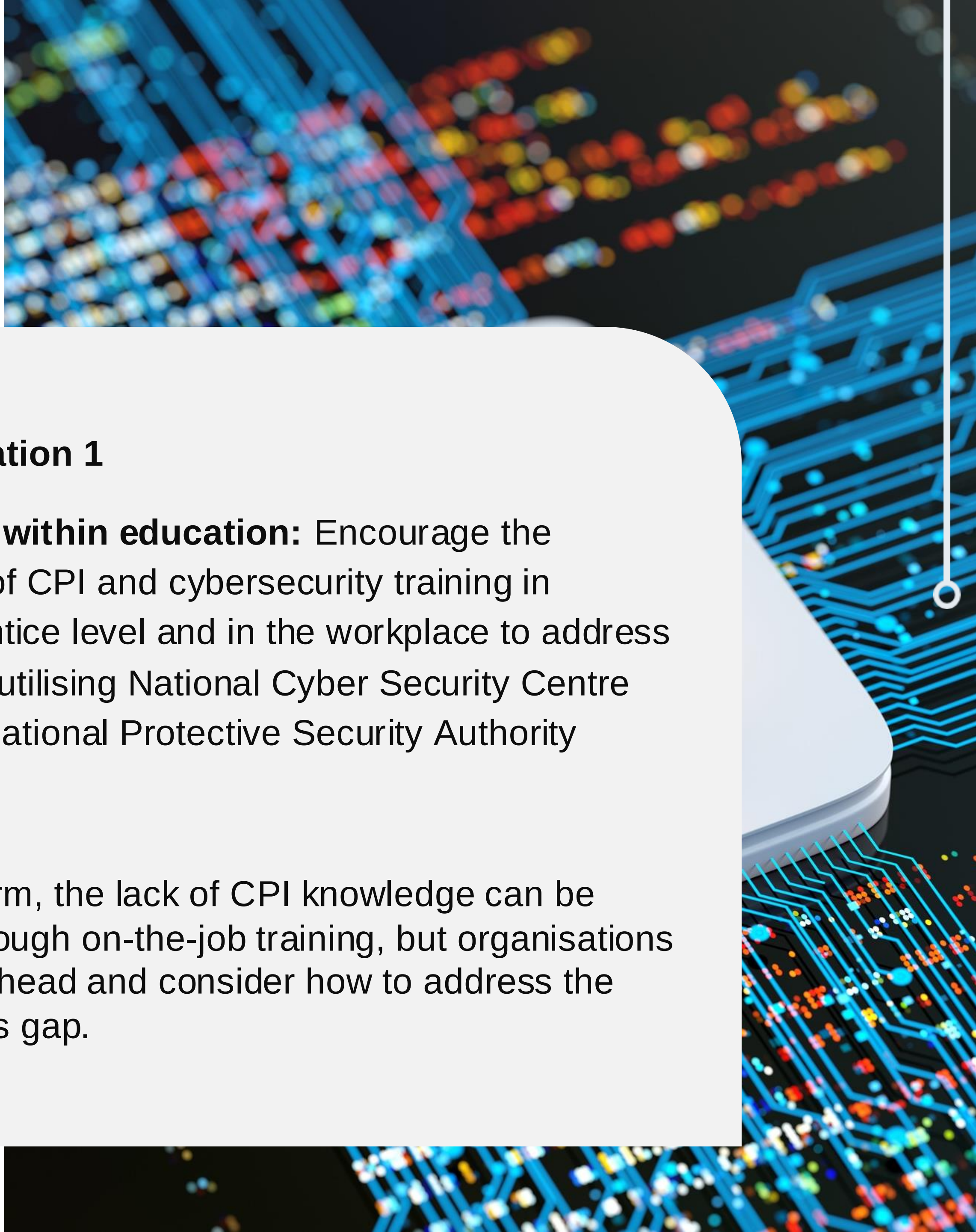
RECOMMENDATIONS

Strategic actions for building resilience and security

Outline recommendations from the workshop to the Department for Science, Innovation and Technology (DSIT), for further consideration through interviews

Traditional technical and operational degrees such as engineering do not include or require students to undertake cybersecurity or cyber-physical infrastructure modules, leaving graduates unequipped to approach security issues relating to connected systems holistically.

Similarly, organisations are increasingly relying on an internet connection and digital storage for information shared across organisations.



Recommendation 1

Integrate CPI within education: Encourage the development of CPI and cybersecurity training in degree/apprentice level and in the workplace to address training gaps, utilising National Cyber Security Centre (NCSC) and National Protective Security Authority programmes.

In the short term, the lack of CPI knowledge can be addressed through on-the-job training, but organisations need to look ahead and consider how to address the long-term skills gap.

RECOMMENDATIONS

Strategic actions for building resilience and security

Outline recommendations from the workshop to the Department for Science, Innovation and Technology (DSIT), for further consideration through interviews

To improve consistency in security standards, a review of the ISA/IEC 62443 series of standards is recommended. The ISA/IEC 62443 series is a set of cybersecurity guidelines for industrial automation and control systems (IACS). The base level of this standard is not fit for purpose, and while the higher levels do achieve some degree of security, the way these are understood (see recommendation one) and procured vary dependent on knowledge, the request, but also on picking the best option based on funding.

Recommendation 2

Apply cybersecurity regulations uniformly within each sector and ensure consistent security standards.

The uniform application of cybersecurity regulations can be improved through the creation of case studies within each sector to share learnings rather than a siloed approach. In the UK, the ACE-CSR is a good example of industry and academic partnerships fostering sharing of information which could be utilised.

RECOMMENDATIONS

Strategic actions for building resilience and security

Outline recommendations from the workshop to the Department for Science, Innovation and Technology (DSIT), for further consideration through interviews

The NCSC has released their own CPI research problem book identifying 6 key problems that require exploration and significant collaborative effort from multiple and diverse stakeholders over the next decade.

Sharing insight and information with members of the public at a time of crisis is seen as a necessary first step in the battle of misinformation.

It is recommended that the UK explore the opportunity to bring sectors together to understand potential cascading failures across the board and test response plans.

Recommendation 3

Promote R&D into CPI: Invest in cross-technology pollination programmes that lead to innovative solutions and support R&D to mitigate risks in emerging technologies (rather than singular tech focus areas)

Recommendation 4

Support public awareness campaigns: Launch campaigns to increase public awareness of CPI threats and foster a culture of security and resilience as fundamental as health and safety.

Recommendation 5

Resilience testing: Enhance and encourage comprehensive resilience testing of critical systems within CPI, including regular testing cycles.