Building Resilience in the Age of AI

How deep tech is strengthening cybersecurity and fraud prevention

Heather Lowrie, Resilionix Limited

Heather Lowrie #WhoAmI

25+ years in tech and cyber/ infosec roles including...

Advisor, Advisory Board Member, Founder
Chief Information Security Officer
Head of Cyber Security, Risk and Resilience
Head of Security, Risk and Resilience
Lead Security Architect
Vice President, Global Technology Risk Governance
Senior Consultant (Payments, Tech Risk, Financial Crime)
Consultant, Research Fellow, Student
Technical Specialist
Technical Team Leader
Software Engineer, Senior Software Engineer
Graduate Trainee

Professional Member of the British Computer Society

The rise of AI-driven cyberattacks and sophisticated fraud tactics - such as deepfake scams and advanced social engineering - are pushing businesses to rethink their resilience strategies, particularly in the context of strategic long-term planning.

In an era where AI is both a tool and a threat, how can you safeguard the future of your organisation and stay ahead of emerging risks?

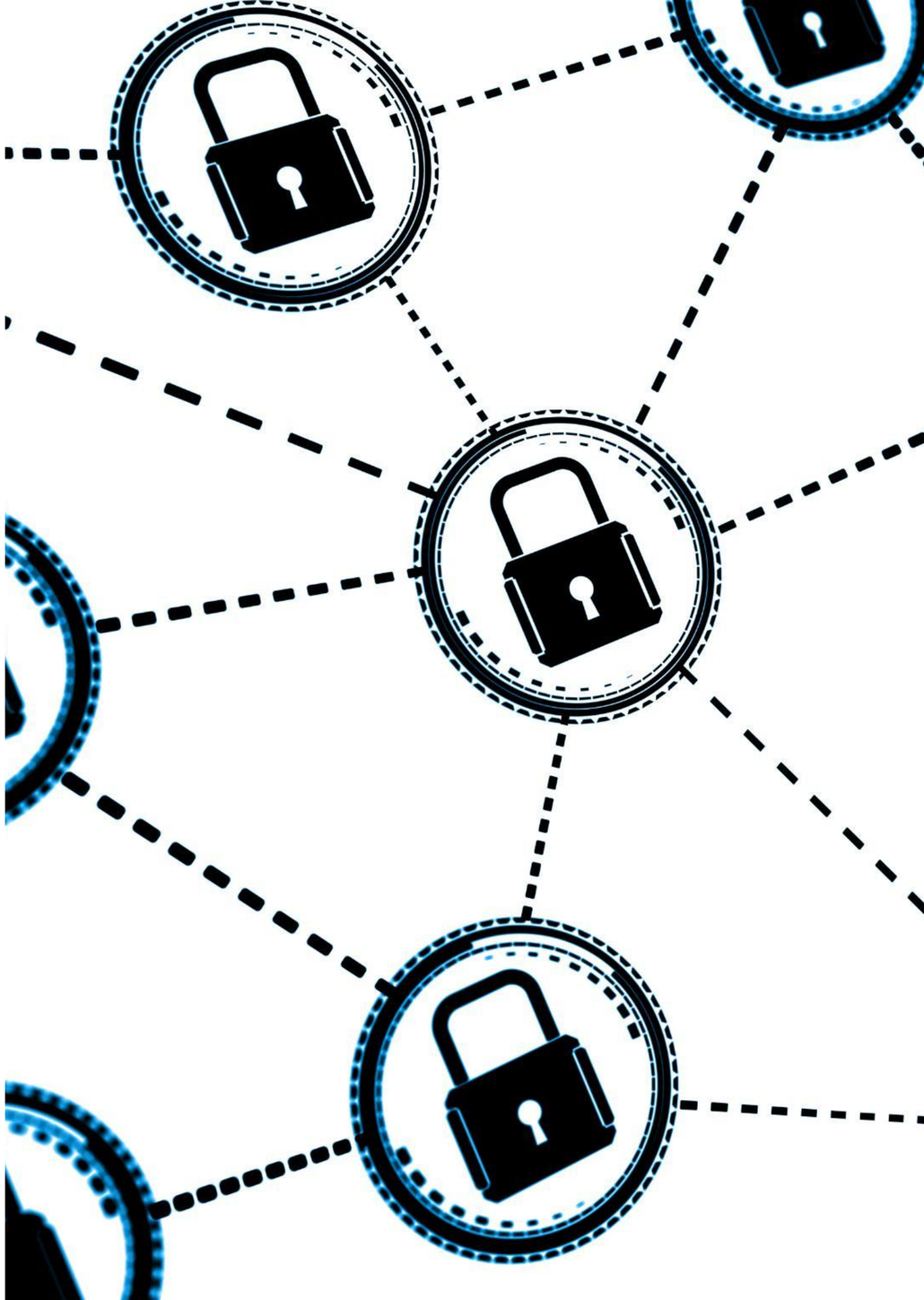
1. Building Resilience

AI-driven cyberattacks and sophisticated fraud tactics

AI-powered mis- and disinformation at scale

Deepfake scams

Advanced social engineering

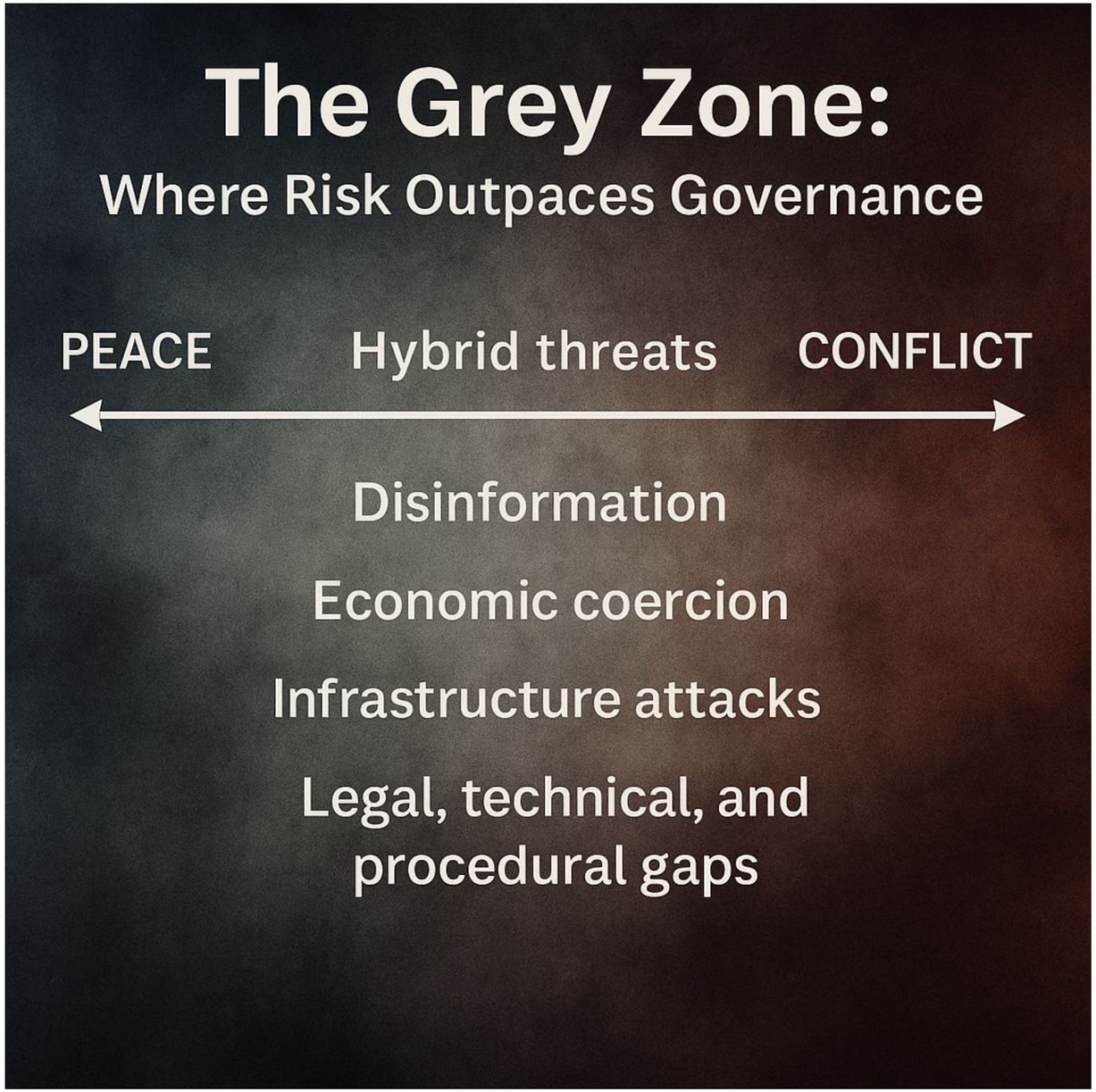


AI: Tool, Threat, or Turning Point?

- AI enables precision, speed, and scale across business and threat activity.
- Emerging risks include synthetic media, data poisoning, and autonomous decision loops.
- The challenge: harnessing potential while mitigating harm.

The Grey Zone: Where Risk Outpaces Governance

- Hybrid threats exploit legal, technical, and procedural gaps.
- Civilian institutions are now targets - healthcare, elections, education, utilities.
- Legacy governance frameworks struggle to adapt.



Why compromise a system when you can compromise trust?

2. Cognitive Resilience

What if…

We could build cognitive resilience in people?

We could build systems for trust and verification?

We led with calm, credible communication?

Cognitive security was a design principle?

Cognitive security is no longer niche; it is a core pillar of modern cybersecurity.

Cognitive Resilience as the First Line of Defence

Teach people to question sources and spot manipulation cues (e.g. unnatural speech, lighting, or context mismatch).

Use scenario-based training to simulate fraud attempts (deepfakes, phishing, synthetic voice scams).

Encourage curiosity over panic: “Pause, Probe, then Proceed.”

Digital literacy is the new civic skill.

Boost situational awareness

Build cognitive habits to slow down automatic trust responses.

Encourage multi-source verification as a daily practice.

Strengthen pattern recognition through exposure to known fraud tactics.

Sense-making under pressure is key.

Stay Grounded

Support emotional regulation so people don’t fall for fear- or urgency-based manipulation.

Create safe channels for second opinions and escalation.

Reinforce shared values and reliable signals (e.g. verified contacts, agreed protocols) to reduce susceptibility to synthetic deception.

Resilience is the foundation of trust.

3. Resilience by Design

Deep Tech in Action: Strengthening Defence and Detection

Behavioural AI: Detects anomalies across identity, transaction, and access patterns in real time.

Graph analytics: Maps complex fraud networks and uncovers hidden relationships.

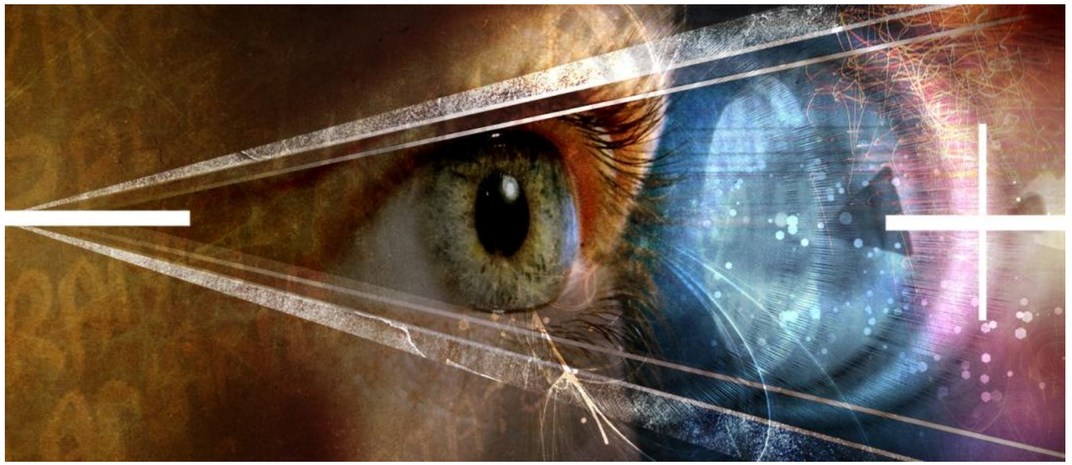
Privacy-enhancing technologies: Data-centric security to protect sensitive data during analysis using techniques like encryption-in-use and differential privacy.

Secure multi-party computation: Enables joint analysis across multiple parties without exposing underlying data for cross-border, multi-entity fraud and threat detection.

Orchestration and Autonomous Response: AI for threat detection and automation for containment and remediation.

Anticipatory Governance

“Governance with foresight” - tackling the next problem, not just the current one.



This Photo by Unknown Author is licensed under CC BY

Antifragile: Building the right foundations for resilience.

Anticipatory: Improving future-preparedness to navigate uncertainty.

Agility: Responding to whatever futures emerge.

Anticipatory governance can help us with unpredictability | World Economic Forum

UK Cyber Governance Code of Practice

Elevating Cyber Governance: UK's Code of Practice Initiative | LinkedIn

- A: Risk Management
- B: Strategy
- C: People
- D: Incident Planning, Response and Recovery
- E: Assurance and Oversight

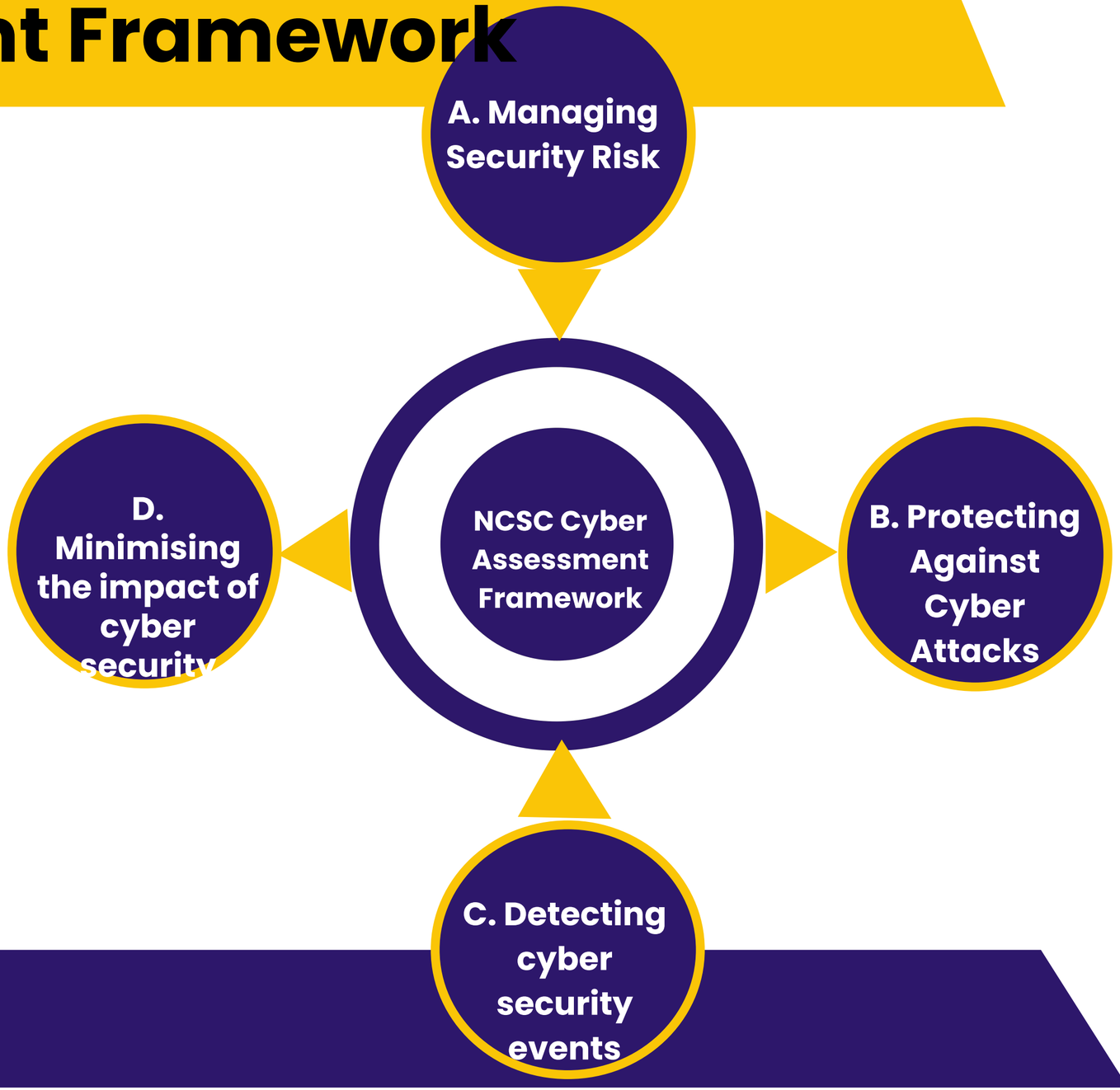
The Cyber Governance Code of Practice is the foundational code in DSIT's modular approach to cyber security codes of practice. It sets out how boards and directors should govern cyber risk. This is complemented by Cyber Essentials, a government backed certification scheme that helps organisations implement fundamental, cyber security controls. Though it is not a code, Cyber Essentials, together with the Cyber Governance Code of Practice, set out the minimum standard that organisations should have in place to manage their cyber risk.

NCSC Cyber Assessment Framework

Cyber Assessment Framework (CAF)

The NCSC Cyber Assessment Framework (CAF) provides a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation responsible.

CAF-based assessments can be carried out either by the responsible organisation itself (self-assessment) or by an independent external entity, possibly a regulator / cyber oversight body or a suitably qualified organisation acting on behalf of a regulator, such as an NCSC assured commercial service



Thank You.