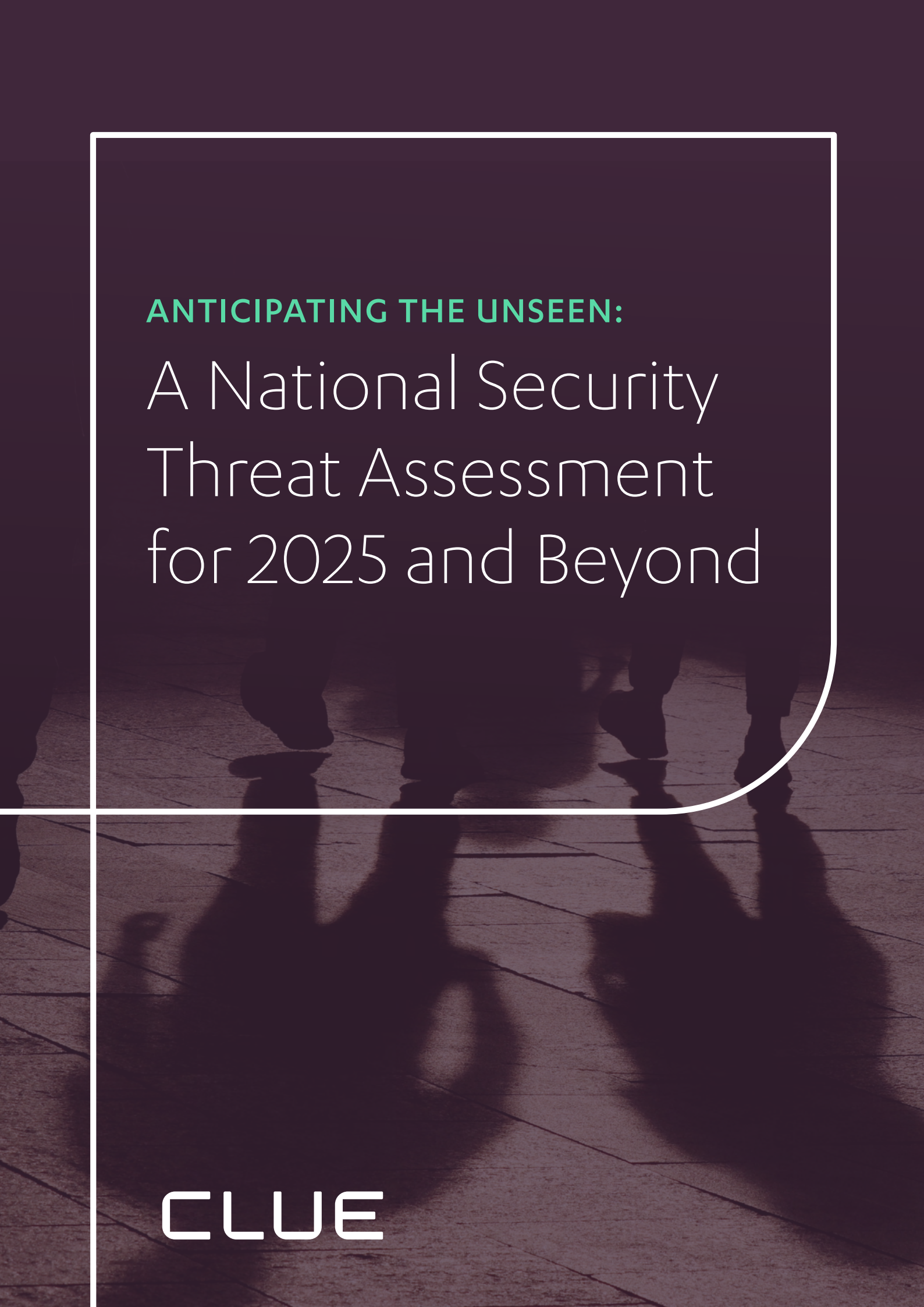

ANTICIPATING THE UNSEEN:

A National Security Threat Assessment for 2025 and Beyond

CLUE

FOREWORD

In over 30 years of national security and law enforcement experience, I have witnessed the evolution of threat landscapes across every domain. But never before have we faced a convergence of such scale and complexity.

The fusion of hostile state threats, technological acceleration, organised and economic crime networks, radicalisation, extremism, and environmental insecurity has created a volatile and unpredictable security environment. As outlined in the UK Government's National Security Strategy 2025 (NSS 2025), we are operating in an era of radical uncertainty - with strategic competition intensifying and threats becoming more hybrid, persistent, and asymmetric.

Today, threats are no longer constrained by geography, nor are they confined to a single form. A cyberattack on a hospital, disinformation targeting an institution, physical attacks via proxies, or the sabotage of undersea infrastructure may all stem from the same hostile actor. These threats cross boundaries, challenge assumptions, and outpace legacy response systems.

The national mission is clear: to disrupt emerging threats before they inflict harm, and to deter aggression through strength. That requires agile, intelligence-led operations, seamless collaboration across public and private sectors, and the technological infrastructure to connect data, insights, and actions in real time. National security is no longer the sole domain of government. It is a shared responsibility.

This Assessment outlines the major trends shaping the UK's threat landscape in 2025 and beyond. It draws on operational insights from law enforcement, intelligence agencies, and technology leaders to deliver a practical assessment of risks and the strategies needed to mitigate them. Many of these trends have been underscored within the UK Government's NSS 2025, including its new strategic framework of Security at Home, Strength Abroad, and Sovereign Capabilities.

As you'll see, resilience in this new era means thinking and acting differently. It means moving from a reactive model to a proactive posture. Because in today's world, resilience is not a luxury. It is a national imperative.

Matt Horne
Director of Intelligence and Investigations, Clue Software & Chair of National Security Committee, techUK

INTRODUCTION

An era of converging threats

Following the release of the NSS 2025, the United Kingdom stands at a critical juncture and the national security threat landscape is more interconnected and complex than at any point in modern history. Traditional categories of threat - terrorism, espionage, cybercrime, and organised crime - are converging and reinforcing each other through shared technologies, overlapping motivations, and blurred allegiances.

State and non-state actors are increasingly collaborating, wittingly or otherwise. Cyber tools developed by criminals are repurposed by hostile states. Organised crime groups facilitate illegal migration or drug trafficking for profit but can also be recruited as proxies for hostile state entities. AI-generated disinformation targets public trust across institutions, simultaneously aiding foreign adversaries and extremist movements.

At the same time, climate change, geopolitical realignments, and economic instability are compounding pressures on public services, infrastructure, and cohesion. The NSS 2025 recognises that the UK must now prepare for both indirect and potentially direct confrontation - and that economic security and social stability are now core pillars of national defence.

This report outlines key threat areas, sector-specific impacts, and practical resilience measures. It is designed to support decision-makers across government, law enforcement, industry, education, and civil society.

Hostile states are operating with greater boldness in the grey zone, using deniable and hybrid tactics to target UK interests

Technological adoption, and acceleration, including AI, is enabling radicalisation, cybercrime, hostile influence, and espionage at scale.

Organised crime and cyber-crime groups are increasingly entangled with state proxies and using sophisticated digital infrastructure.

Climate insecurity and geopolitical volatility are compounding strategic fragility at home and abroad.

Cross-sector coordination, integrated intelligence, and real-time resilience are the most urgent operational priorities.

The threat landscape in 2025 and beyond

Hostile states and hybrid threats:

The rise of state aggression below the threshold of war has driven a resurgence of grey zone tactics, with Russia, China, Iran, and North Korea all leveraging covert and deniable methods to undermine UK interests. These states exploit proxy actors, economic coercion, and hybrid operations to disrupt critical infrastructure and erode institutional trust.

China continues to pursue long-term strategic advantage through intellectual property theft, academic and industrial espionage, and the infiltration of sensitive research sectors - particularly in AI, quantum, and biotech. Iran, meanwhile, has intensified its targeting of UK-based dissidents, launched repeated cyber intrusions into public sector systems, and supported plots intended to sow fear and destabilisation on UK soil.

Tactics used by hostile states include:

- Espionage and infiltration of research, academic, and commercial institutions
- Disinformation and influence operations to manipulate public discourse
- Disruption of infrastructure, including telecoms and energy networks
- Collaboration with organised crime for sanctions evasion and covert financial flows

The exposure of the Russia-backed 'Minions' proxy network and the sabotage of Baltic subsea cables highlight an escalating willingness by adversaries to operate within UK borders. This signals a new phase of hybrid confrontation - one that directly challenges national resilience, economic stability, and sovereignty in both digital and physical domains.

48% increase in espionage activity targeting the UK in the past year, according to MI5[1]

MI5 foiled 20 Iran-backed plots since January 2022, many aimed at UK-based dissidents[2]

Undersea internet cables and telecoms now flagged as high-risk critical infrastructure due to sabotage and cyberattack concerns[3]

Case Study

'The Minions': GRU-backed espionage ring operating in UK

A UK-based Bulgarian spy cell dubbed 'The Minions' led by Orlin Roussev and directed by fugitive ex-Wirecard COO Jan Marsalek, acted as a conduit for Russian intelligence (GRU/FSB). Communicating via encrypted Telegram, the group conducted surveillance on Kremlin critics and planned operations against Ukrainian soldiers abroad. Espionage tools included tracking devices and disguises.

Six operatives were convicted in May 2025 and sentenced to up to 10 years in prison. This case highlights a growing trend: hostile states outsourcing espionage to proxy operatives to avoid diplomatic exposure and operate transnationally.

[1] reuters.com/world/uk/russias-gru-seeking-cause-mayhem-britain-europe-uks-mi5-spy-chief-says-2024-10-08
[2] hansard.parliament.uk/Lords/2025-03-06/debates/0AD4E229-2565-490E-AFEF-BC79846589BE/IranianStateThreats
[3] commonslibrary.parliament.uk/seabed-warfare-protecting-the-uks-undersea-infrastructure

Cyber, AI and encryption threats

Cyberattacks are increasing in both scale and sophistication, with hostile actors now probing the UK's digital infrastructure on a near-continuous basis. Government reporting confirms that critical national systems are subject to daily operations by states including Russia and Iran, with public services, utilities, and logistics frequently targeted.

The National Cyber Security Centre (NCSC) has urged a strategic policy response, including updated legislation to drive the development of secure, resilient technologies. In 2024, the UK recorded a 16% rise in serious cyber incidents, with 430 high-impact attacks targeting:

- AI and machine learning platforms
- Health and education systems
- Critical supply chains and logistics
- Encrypted communication services

Beyond technical threats, hostile actors and extremist groups are increasingly using digital platforms for ideological influence. Social media, encrypted apps, and online forums have become accelerators of radicalisation – enabling anonymous grooming, recruitment, and coordination. In 2024, 78% of known radicalisation pathways began online, aided by algorithmic targeting and AI-generated propaganda.

Quantum computing also poses a looming threat. Its decryption capabilities could undermine secure communications, financial systems, and critical infrastructure. The UK must prioritise investment in post-quantum encryption, cybersecurity standards, and digital identity frameworks.

Artificial intelligence is now a powerful force multiplier. It is already being used to create deepfakes, automate phishing, impersonate officials, and generate malicious code. Emerging risks include autonomous malware, model poisoning, and synthetic identities – tools already in use by hostile states, organised crime groups, and extremist networks.

Without effective regulation, algorithmic accountability, and security-by-design standards, AI risks outpacing national defences. Governments, developers, and digital platforms must treat AI not only as an innovation challenge – but as a core security priority.

- 430 serious cyber incidents in 2024 (+16% YoY)[4]
- 78% of radicalisation pathways now begin online (Gov.UK)[5]
- 3 of the 5 largest ransomware attacks in 2024 targeted UK healthcare[6]

[4] ncsc.gov.uk/files/NCSC_Annual_Review_2024.pdf
[5] assets.publishing.service.gov.uk/media/638f089bd3bf7f327e1ea969/internet-radicalisation-report.pdf
[6] periculo.co.uk/cyber-security-blog/post/nhs-cyber-attacks-and-incidents-in-2024

Economic crime and Organised Crime Groups

Organised Crime Groups (OCGs) remain primarily financially motivated enterprises, driven by the pursuit of profit, asset accumulation, and local or transnational dominance. Their main activities are centred on illegal commodities, illicit markets, fraud, and the laundering of criminal proceeds.

However, a small but significant subset of these groups are being opportunistically recruited or exploited by hostile state actors as proxies - particularly where their capabilities in financial systems, digital infrastructure, or illicit logistics can serve broader geopolitical goals.Increasingly, OCGs:

- Collaborate across national borders and ethnic lines to optimise illicit supply chains
- Exploit cryptocurrency and informal value transfer systems (e.g., hawala) for moving and laundering funds
- Use encrypted communications and dark web marketplaces to operate with greater security and anonymity

These groups continue to launder profits through complex offshore networks and cryptocurrency, often facilitated by shell companies and complicit or negligent financial enablers. Joint operations between the NCA and international partners have shown that crypto-enabled laundering is now a common feature in cases involving hostile state interests. In 2024, an NCA operation in cooperation with the FBI, DEA, OFAC as part of Operation Destabilise resulted in the seizure of over £20 million in cash and cryptocurrency from laundering networks linked to organised crime, ransomware groups, Russian intelligence and espionage efforts.

While the majority of OCGs operate independently for financial gain, the increasing convergence of organised crime and state-aligned threat actors - especially in sanctions evasion, espionage logistics, and influence operations - represents a strategic security concern.

59,000+ individuals currently involved in organised crime across the UK [7]

Serious organised crime costs the UK £47 billion annually (drug supply £26 bn; economic crime £11 bn) [8]

Case Study

Operation Destabilise - £20 million disrupted in crypto laundering network

In 2024, the UK's National Crime Agency disrupted over £20 million in cash and cryptocurrency linked to a sprawling Russian-speaking money laundering network. Two criminal groups, Smart and TGR, provided laundering services to drug gangs, ransomware groups, and sanctioned Russian elites.

The laundered funds enabled espionage, property purchases, and disinformation operations. Using cash couriers and USDT stablecoins, the network blended traditional and digital methods to bypass sanctions and financial scrutiny. The case exposed direct links between organised crime and Russian state activity - demonstrating how crypto-finance now underpins hostile state operations and highlighting major national security vulnerabilities.

[7] [8] gov.uk/government/news/new-strategy-to-tackle-organised-crime

Climate, resources, and strategic fragility

Climate disruption is no longer a future threat - it's an active multiplier of geopolitical instability, resource scarcity, and domestic emergency strain. It is driving:

- Regional instability and mass displacement
- Competition for water, food, and critical minerals
- Emergency response fatigue and resource diversion

UK interests are increasingly exposed abroad - in fragile states and global supply chains - while domestic infrastructure faces climate-linked vulnerabilities such as flooding, heatwaves, and wildfire, which could be exploited by adversaries to stretch emergency services or criticise government response.

The 2022 UK heatwaves resulted in nearly 3,000 excess deaths, primarily among elderly populations, according to the UK government, while the UK Green Building Council warns that many schools, offices, and care homes are not equipped to handle projected heat and infrastructure stress.

Meanwhile, over 2 million people in England now live in flood-prone zones, according to the National Fire Chiefs Council (NFCC), a figure expected to rise by 60% by 2050.

Nearly 2 million people and one-third of critical infrastructure are currently at flood risk[8]

Buildings, including schools and care homes, are largely unprepared for escalating climate impact[9]

Heatwaves in 2022 caused nearly 3,000 excess deaths, mainly among vulnerable populations[10]

[8] publicfirst.co.uk/wp-content/uploads/2025/03/From-risk-to-resilience-report_PF_200325.pdf
[9] theguardian.com/environment/2025/jun/26/uk-care-homes-schools-and-offices-not-equipped-to-deal-with-global-heating
[10] ons.gov.uk/peoplepopulationandcommunity/birthsdeathsandmarriages/deaths/articles/excessmortalityduringheatperiods/englandandwales1juneto31august2022

image by John Barker

Who is at risk?

Examples of cross-sector threat exposure:

Government
Cyber intrusion, disinformation, insider threats

Healthcare
Ransomware, data theft, infrastructure sabotage

Finance
Sanctions evasion, crypto laundering, fraud

Education
Campus espionage, radicalisation, IP theft

Sport
Political signalling, extremism at high-profile events

CNI/Utilities
System disruption, hybrid interference, resource targeting

Intelligence infrastructure for a connected threat landscape

Today's national security threats evolve too quickly and operate too broadly for siloed, reactive systems to keep pace. From cyber-enabled espionage and state-backed sabotage to organised crime and insider threats, the UK requires intelligence infrastructure that can surface risks early, connect disparate information, and enable swift, coordinated action.

Modern investigation and intelligence platforms are central to this shift. These tools support secure case management, real-time intelligence sharing, and multi-agency collaboration. They help organisations detect emerging threats, map complex actor relationships, and accelerate decision-making across high-risk domains such as border security, critical infrastructure, and financial crime.

The strength of these platforms lies not in replacing human judgement, but in enhancing it – offering speed, structure, and insight at scale. Building this capability across government, policing, and civil society is essential to sustaining resilience and disrupting threats before they escalate.

> The UK requires intelligence infrastructure that can surface risks early

International coordination and strategic alliances

The UK's national security does not exist in isolation. In 2025, most serious threats – including cyber attacks, illicit finance, disinformation, and organised criminal networks – operate across borders.

To deter and disrupt these, the UK must strengthen its international partnerships and align operational capabilities with its allies.

Intelligence-sharing arrangements such as the Five Eyes alliance provide critical visibility into global threat activity. Collaborative frameworks through NATO, Europol, Interpol, and the UN enable joint planning, sanctions enforcement, cyber response, and counterterrorism operations.

As adversaries become more agile and networked, so too must the UK and its partners. Greater legal, technical, and operational alignment – including secure data-sharing platforms, shared exercises, and multilateral intelligence coordination – will improve collective resilience and give the UK strategic depth in a contested global environment.

> As adversaries become more agile and networked, so too must the UK and its partners.

What you can do to protect your organisation – and UK national security

National security is no longer the sole responsibility of government. Every organisation plays a vital role in building resilience and protecting the nation. The actions below can help strengthen your defences and align with national objectives.

1. Assess your risk

- Map critical assets: Identify your organisation's crown jewels – sensitive data, operational technology, key personnel, and supply dependencies.
- Profile your threat exposure: Include cyber intrusion, espionage, insider risk, disinformation, supply chain disruption, and climate hazards.
- Refresh regularly: Reassess threats quarterly or after major incidents. Use horizon scanning to account for AI-driven threats, geopolitical flashpoints, and systemic vulnerabilities.

Practical Tip: Run a tabletop risk review session with senior leaders and key departments (IT, legal, ops) to align awareness and prioritise risks.

2. Secure your systems

- Establish cyber hygiene as standard: Enforce multi-factor authentication across all accounts, ensure all systems are patched within 7 days of release, and isolate backups from your main network.
- Tailored training: Implement short, role-based cyber awareness modules. Focus on frontline risks (e.g. phishing for staff, privilege misuse for admins).
- Test your response: Simulate a cyberattack or data breach with a red team or tabletop exercise. Identify bottlenecks in escalation, decision-making, or legal response.

Practical Tip: Use the Cyber Essentials checklist as a starting point and assign responsibility for each domain (access control, patching, backups, etc.).

3. Collaborate & share intelligence

- Monitor threat intelligence: Subscribe to alerts from NCSC, your sector regulator, or commercial threat intel providers. Make sure someone reads and acts on them.
- Join a trusted network: Engage with your sector's ISAC or join a local resilience forum. Contribute observations – not just consume updates.
- Nominate a threat lead: Appoint a named individual (or small team) responsible for reviewing threat data, coordinating internal alerts, and liaising with authorities when needed.

Practical Tip: Use secure tools (not email) to circulate alerts internally. Consider creating a monthly "threat bulletin" for execs or ops teams.

4. Plan for disruption – inside and out

- Hybrid scenarios: Prepare for complex events – a cyberattack during a protest, a data breach during a climate emergency, or insider sabotage during peak season.
- Mitigate insider threats: Conduct regular access reviews, set up clear and confidential reporting channels, and train HR/IT/legal to spot red flags (e.g., sudden behaviour changes, offboarding anomalies).
- Secure your supply chain: Audit vendors for cybersecurity posture, data handling practices, and geopolitical exposure. Embed breach notification and continuity clauses into contracts.
- Boost climate readiness: Test how operations would continue if buildings, power, or transport were disrupted. Stock critical spares, prepare remote access contingencies, and coordinate with emergency services.

Practical Tip: Use a "resilience checklist" across departments and ask each to develop a fallback plan for their core services.

5. Align with the UK's National Security Strategy

- Support sovereign capabilities: Prioritise UK-based tech, manufacturing, and talent where possible.
- Comply with national standards: Follow NCSC guidance, meet regulatory expectations (e.g. DSPT, ISO 27001), and monitor updates to critical national infrastructure policies.
- Engage with government support: Leverage funding, guidance and partnerships from bodies like NCSC, DSIT, Innovate UK, and local resilience hubs.

Practical Tip: Appoint a liaison to track relevant national initiatives and funding calls – and feed these into your security and innovation planning.

Key conclusions

The threat landscape is converging fast.

Traditional categories like cyber, crime, espionage, and extremism are no longer separate – they overlap and reinforce each other.

State and non-state actors are fusing.

Hostile states use criminal proxies, disinformation networks, and localised disruption to undermine the UK from within.

Siloed systems can't cope.

Fragmented, reactive approaches are too slow for today's threats. Coordination and real-time response are critical.

Intelligence and collaboration are strategic imperatives.

Investing in secure platforms, cross-sector intelligence sharing, and public-private partnerships is no longer optional – it's foundational to national resilience.

FINAL WORD:

From reaction to resilience

The UK faces a period of sustained strategic pressure. Responding effectively will depend not only on identifying threats, but on disrupting them before they inflict harm. This demands a clear shift – from fragmented, reactive postures to integrated, intelligence-led strategies.

Solutions that unify intelligence, link insight to action, and support secure coordination – such as Clue – are enabling this transition across government and critical sectors. They represent more than a technical fix; they are foundational to a faster, more efficient and resilient approach to national security.

The threats are real and immediate. But so too is the opportunity to act decisively – and build the infrastructure, alliances, and foresight that will define the UK's strength in the years ahead.

To learn more about how Clue is supporting organisations in protecting national security, visit: **www.cluesoftware.com/national-security/**

Read our latest threat assessments

Securing the UK's Maritime and Border Domains

Our report Securing the Maritime and Border Domain, explores some of the most pressing threats to the UK's security, and how agencies can respond more effectively with intelligence-led tools and collaboration.

Access here:
cluesoftware.com/maritime-and-border-security

Insider Threat Assessment for 2025

Our Insider Threat Assessment, explains the rise in insider risk and why traditional security no longer suffices. It outlines an intelligence-led approach to detection and prevention, from national security breaches to ransomware.

Access here:
cluesoftware.com/insider-threat

CLUE

Clue House, Petherton Road, Hengrove, Bristol, BS14 9BZ, UK.
Company Number 01715616
Company registered in England & Wales.