

Navigating the Cyber Grey Zone: Geopolitics, Agentic AI, and the UK's Strategic Response

Protecting our National Infrastructure at Machine Speed

Giles Grant

CEO

UK Cyber Security Council



Department for
Science, Innovation
& Technology



National Cyber
Security Centre



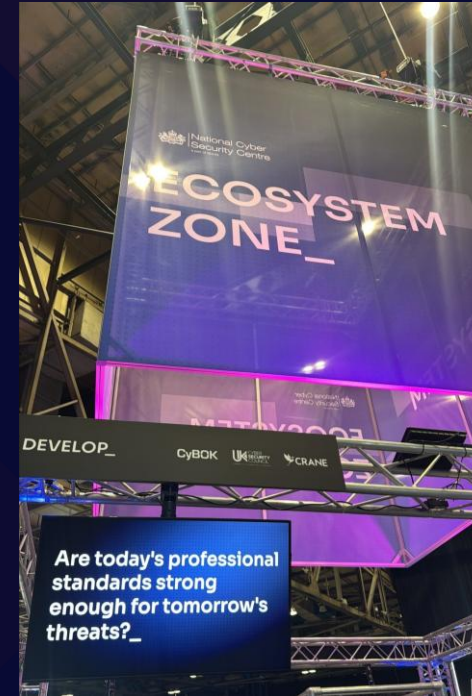
GCHQ

What is the UK Cyber Security Council?

The UK Cyber Security Council is the independent chartered professional body for the UK's Cyber Security Sector under Royal Charter.

We exist to **CONNECT**, **CHAMPION** and **CHARTER** the cyber security profession – all with the goal of making the UK the safest place to life and work online.

Through **setting the standards for industry competence and ethics**, holding the **Cyber Security Professional Register** and **encouraging more people to get into a career in cyber**, we're on a mission to grow and empower the UK's cyber security workforce.



The History of the Council



2016: National Cyber Security Strategy highlighted the need for professionalisation of cyber security.



2016-2021: Project to form UK Cyber Security Council undertaken, involving government, industry, academia and professional bodies from closely related disciplines (Engineering, IT, Information Security).



2021: UK Cyber Security Council granted Royal Charter.



2022: First professionals granted Chartered Cyber Security Professional (ChCSP) title.



2023: Professional registration open to all.

What We Do

- **We set the standards for the cyber security profession** through the UK Cyber Security Standard for Professional Competence and Commitment.
- Our Royal Charter status enables us to **award Professional Cyber Security Titles** and hold the UK's Cyber Security Professional Register.
- **We support people to start their career in cyber** providing resources, webinars and networking opportunities to demystify routes into and through the sector.
- As the sector's self-regulatory body, **we set codes of ethics and professionalism** and provide other governance and oversight functions where appropriate.
- **We share knowledge across the sector** bringing together thought leaders, running insightful events and connecting professionals with employers.

Navigating the Cyber Grey Zone: Geopolitics, Agentic AI, and the UK's Strategic Response

Protecting our National Infrastructure at Machine Speed



The New Security Reality

- **Rapid Threat Shift:** Frontier AI (Mythos 5, Fable 5), Geopolitical friction (Russia, China, North Korea), and state-empowered Organized Crime.
- **Rising Incident Volume:** NCSC reports ~200 serious incidents, a +50% increase from last year.
- **Data over Definitions:** Cybersecurity is no longer just IT; it is the convergence of people, process, and technology to defend national capability.

Lessons from the Battlefield

- **Welcome to the “Grey Zone”:** Operating in the active space between war and peace.
- **Pace and Dominance:** Operating at machine speed; localized dominance over absolute control.
- **The Widening Target:** Adversaries are bypassing the frontline, targeting national infrastructure and commercial supply chains.

The Agentic AI Arms Race – a paradigm shift

- **Abstract to Tangible:** Agentic AI is fundamentally altering intelligence and defence capabilities.
- **The Global Race:** Frontier models primarily US-led, accelerating a "compute, baby, compute" mindset.
- **The Open-Source Variable:** Open-source models moving rapidly at a fraction of the cost, democratizing advanced capabilities.

A Shifting Global Order

- **US Realignment:** A profound reassessment of the US's traditional global posture.
- **Intelligence Silos:** Agentic AI capabilities altering Five Eyes sharing dynamics.
- **Eroding Rule of Law:** Breakdown of the traditional rules-based order; normalization of coercion and intimidation.

The European Threat Landscape

- **Russia's Hybrid Warfare:** GRU and FSB shifting from battlefield operations to direct attacks on European civilians and infrastructure.
- **Escalating Sabotage:** Targeting Polish energy, French critical national infrastructure, and EU/UK subsea cables.
- **China's Unprecedented Resource:** Aggressive intelligence gathering and infrastructure prepositioning (e.g., Salt Typhoon).

The Solution – A Unified Strategic Response

- **Integrated Defence:** A partnership between Industry, Military, and Government (MoD, GCHQ, NCSC, UKCSC).
- **Four Core Themes:**
 1. Intelligence Sharing
 2. Physical Proximity and Collaboration
 3. Culture and Board-Level Behaviours
 4. Agile Demand and Supply

Raising the National Baseline: The role of the UKCSC

The UKCSC Mission: To professionalize the workforce through national standards in competence and ethics.

- **Why it is Mission-Critical Now:**

- **Tooling vs Defence:** Agentic AI outpaces manual defence.
- **Systemic Risk:** JLR, British Library, and NHS breaches prove cyber is a national capability issue.
- **Simplifying Trust:** Common standards reduce systemic risk in Critical National Infrastructure (CNI) and procurement.
- **Accountability:** Ethical AI practice requires a visible, competent workforce.

UKCSC Professional Registration = UK Economic and Democratic Resilience

The Path Forward – What You Can Do

- **Professionalise Your Teams:** Align and train your security workforce with UKCSC Charters and standards. Join us as an organisation.
- **Train Your Boards:** Ensure leadership understands the systemic nature of cyber risk in the Grey Zone. Rehearse & roll play.
- **Build resilience:** Public & Private sector – accelerate & automate patching programs, ensure access to best-in-class protections to mitigate exposure, establish structural containment, need for near-real-time detection & response.

The Path Forward – What You Can Do

- **Professionalise Your Teams:** Align and train your security workforce with UKCSC Charters and standards.



The Path Forward – What You Can Do

- **Corporate Membership:** Join us as an organisation.



**Thank You
&
Any Questions?**

UK Cyber Security Council



Appendix

Corporate Members

- Affiliation with a trusted brand in cyber security.
- Being seen to support the Council and its mission.
- Promotion through our marketing channels and submitting thought leadership pieces.
- Demonstration that organisations work to high ethical standards through signing our ethical deceleration.

ENHANCED BENEFITS	ONE OFF COST (+VAT)
Social media post (LinkedIn & Twitter)	£300
Newsletter feature	£300
Sponsored blog post	£500
Event badge sponsor	£1,000
Full media package – thought leadership article.	£1,000
Headline webinar sponsor	£1,500

ANNUAL REVENUE	ANNUAL COST
<£1 million	£500
>£1 million	£1,500
>£5 million	£5,000



Elevator Pitch: “The UK Cyber Security Council exists to build a trusted and unified cyber profession, setting the national standard for excellence, ethics, and expertise that empowers professionals, inspires public trust, and strengthens the UK’s digital future”.

VISION

Building a trusted and unified cyber profession. The recognized home of excellence, ethics, and expertise that earns confidence from classrooms to boardrooms and safeguards the UK’s and others digital future.

MISSION

To professionalize the UK’s cyber workforce by setting the national standards for competence and ethics, accrediting individuals and organizations that meet them, and fostering the skills, collaboration, and public trust needed to secure the UK’s digital economy.

UKCSC is mission critical now

Agentic AI and automated tooling are accelerating attacks faster than traditional defences can adapt, and recent UK incidents across automotive, cultural, and health sectors show the risk is systemic. The UK Cyber Security Council raises the national baseline through trusted professional standards, skills pathways, and assurance, simplifying procurement and third-party trust in Critical National Infrastructure and public services while embedding secure-by-design, ethical AI practice, and a visibly competent workforce aligned across government and industry.

Rising threat velocity and autonomy

- Agentic AI and automated tooling accelerate attack discovery, exploitation, and scale, outpacing manual defense.

Systemic exposure across UK economy and public services

- Recent breaches in automotive supply chains, cultural institutions, and health services show cyber is a national capability issue, not just IT.

Need for a trusted professional standard

- A single, coherent framework for competence, ethics, and continuous upskilling raises the baseline across all sectors and suppliers.

Workforce capacity and skills gap

- Clear pathways, accredited specialisms, and a visible register help grow, verify, and mobilise scarce talent where risk is highest.

Assurance for government and critical supply chains

- Common standards simplify procurement, improve third-party assurance, and reduce systemic risk in Critical National Infrastructure and public contracts.

Responsible adoption of AI and data

- Embedding secure-by-design, governance, and professional accountability ensures innovation doesn't outrun safety.

Measurable national resilience

- Council-led metrics on competence, time-to-certify, and incident readiness enable evidence-based policy and investment.

Convening power and ecosystem alignment

- Neutral, Royal Charter authority to align Licensed Bodies, industry, and government around shared outcomes and faster adoption.