THE STATE OF THE CYBER NATION

National Cyber Security Centre

a part of GCHQ

Contents

INTRODUCTION

Foreword: Richard Horne, CEO, NCSC 4
Ministerial foreword 6
Message from Director, GCHQ 8

A VISION FOR THE FUTURE 10

UNDERSTANDING THE THREAT 13
A decade of cyber threat 14
The cyber threat to the UK 17
The impact of AI on cyber threat 21
The age of autonomous attack 24
Incident management 26
7 things we learned 28

TECHNOLOGY AND THE FUTURE OF CYBER SECURITY 31
A decade of technological change 32

BUILDING STRONG FOUNDATIONS 39
Embedding cyber security into everything 40
Why 'building strong foundations' has never mattered more 42

SECURING THE BACKBONE OF SOCIETY 53
A moment of choice 54

THE FUTURE OF CYBER DEFENCE 65
The changing nature of operational cyber defence 66
Building the future of cyber defence 67
Building the UK's agentic cyber defence ecosystem 70
Project DROMOS 74

SHAPING GLOBAL CYBER RESILIENCE 77

Foreword

The UK enters 2027 at a watershed moment.

Over the past decade, we have built world-class cyber security capabilities, established the NCSC as a trusted authority at home and abroad, and strengthened partnerships with government, industry and academia.

Across Scotland, Wales and Northern Ireland, the NCSC expanded its engagement with devolved governments, helping public services, democratic institutions and critical national functions better understand cyber risk and make greater use of NCSC advice, services and expertise.

We can be proud of that progress, and we must also be honest. The UK's cyber resilience is not yet where it should be. The cyber threat has increased faster than our defensive capabilities, leaving too many organisations vulnerable to attacks that could – and should – be prevented.



> The cyber challenge for the next decade is ensuring organisations are adequately prepared and can adapt quickly enough to defend themselves against AI-powered attacks.'

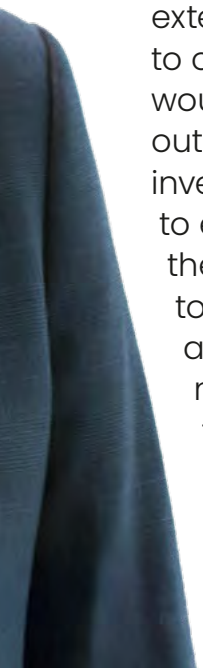
AI brings this reality into sharper focus. AI makes cyber attacks easier, faster and cheaper to execute, and at greater scale. But AI did not *create* these cyber security weaknesses; it *revealed* them. It exposed years of technical debt and the failure to implement even basic cyber protections, with technology and security investments too often deferred.

The biggest cyber security challenge of the next decade requires us to look not at our attackers, but at ourselves.

It is whether organisations can modernise their technologies and build resilience at the pace that's required.

And, there is reason for optimism. AI and the investment path that organisations will take to adopt it, also represents the best opportunity we have to improve cyber security at scale.

Used responsibly, AI can help us identify weaknesses faster, automate defensive actions, accelerate recovery and extend advanced capabilities to organisations for whom they would previously have been out of reach. As organisations invest in developing technology to enable them to adopt AI, they have the opportunity to refresh their technology and build proper full-life maintenance regimes with focus and urgency.



10 years on from the NCSC's formation, we face a moment of choice. If we act now, cyber security can become a source of national strength, driving economic growth and building trust in our increasingly digital world.

If we delay, cyber attacks will become more frequent, more severe and more costly.

The future is not set. The UK's ability to withstand disruption – and to exploit the opportunities that AI promises – will be determined by the choices we make now, the speed with which we adapt, and our collective willingness to act.

This Annual Review is both a reflection on the progress the NCSC has made, and a call to action for the decade ahead. Inside, you'll see that the tools, standards and frameworks that can protect the UK from conventional and AI-powered cyber attacks already exist. The challenge now is quickly implementing these at scale.

Richard Horne,
CEO NCSC

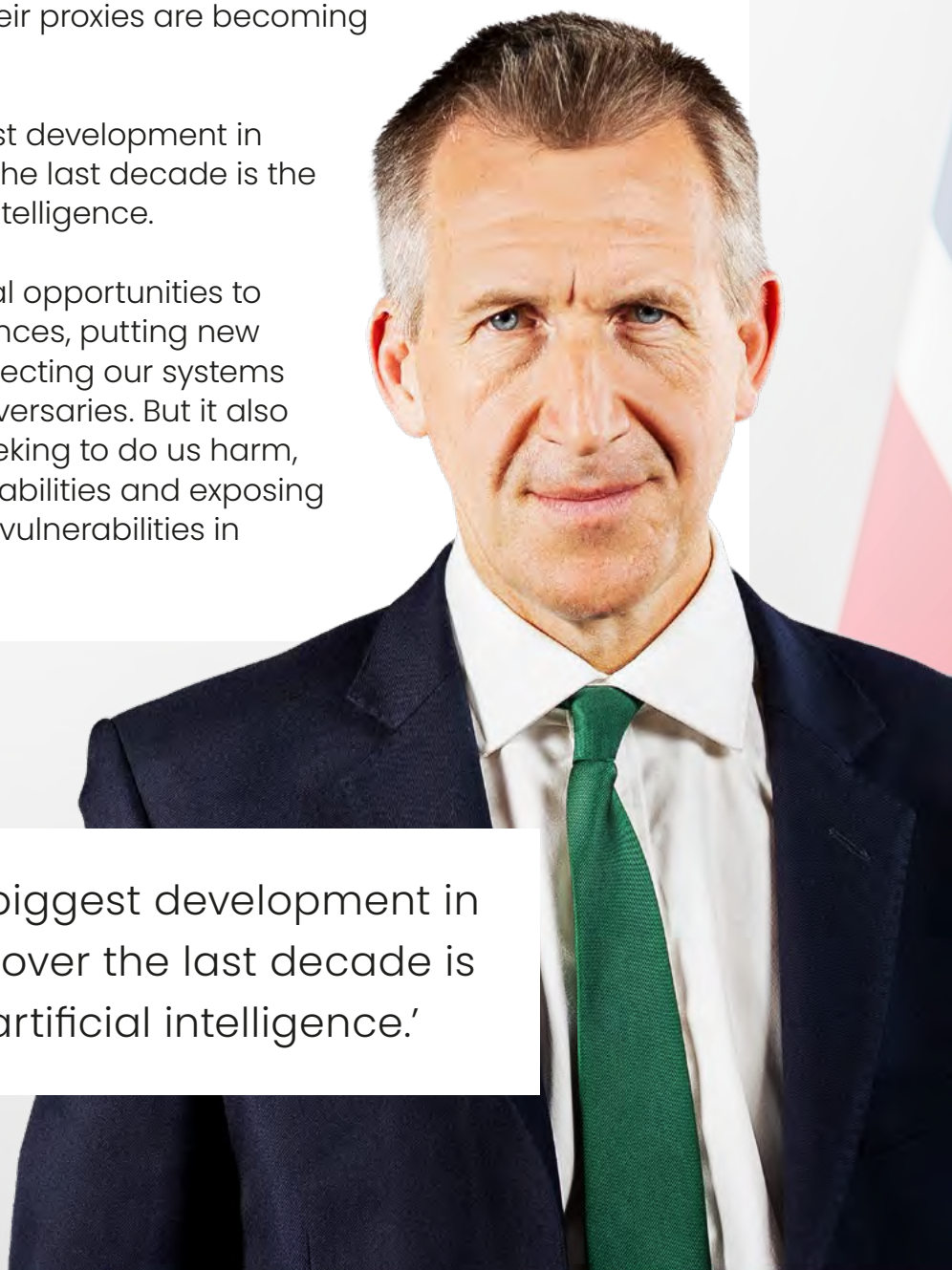
Ministerial foreword

If a week is a long time in politics, then a decade is an epoch in cyber security.

The cyber security landscape has changed considerably since the National Cyber Security Centre opened its doors ten years ago. The raw number of cyber attacks is increasing. State threats and their proxies are becoming more brazen.

But by far the biggest development in cyber security over the last decade is the advent of artificial intelligence.

AI opens up practical opportunities to strengthen our defences, putting new tools to the test, protecting our systems and tracking our adversaries. But it also empowers those seeking to do us harm, upgrading their capabilities and exposing previously unknown vulnerabilities in our defences.



‘But by far the biggest development in cyber security over the last decade is the advent of artificial intelligence.’



Maximising opportunities whilst minimising risks from AI is an era-defining challenge. This year's Annual Review shows the NCSC stands on the frontline of meeting it, as national initiatives like Cyber Shield and the National Detect Strategy are using AI to deliver automated defence at scale.

Government action to respond to fast-changing cyber threats is accelerating too. This government has published the Government Cyber Action Plan – backed by more than £210 million of investment, improving the resilience of public services and our incident response. The National Cyber Action Plan will soon follow, as we continue to progress through the Cyber Security and Resilience Bill, the biggest update to UK cyber regulation in years.

Yet despite the pace of change, I am struck in reading this year's Annual Review that the core components of good cyber security remain exactly the same today as they did in 2016. Familiar and preventable weaknesses like unpatched software and password compromise remain open doors for our adversaries that too many organisations are not taking seriously.

As the NCSC enters its second decade, I express my utmost gratitude for the tireless work it does to keep us safe, every single day. I also encourage businesses and organisations across the UK to step up and play their part in our defences. Implement Cyber Essentials. Sign up to the Cyber Resilience Pledge. Join the NCSC's Early Warning service.

By working together to strengthen the foundations of our cyber security today, we can ensure our country remains secure for the decade ahead.

Dan Jarvis MBE MP,
Minister of State (Minister for Security)

Message from Director GCHQ

In an age of radical uncertainty, contested geopolitics and rapidly changing technology, cyber security must be an urgent priority for all organisations.

Over the past decade, the National Cyber Security Centre has established and continued to evolve and reimagine the role of cyber security and helped organisations and individuals understand cyber risk, respond to incidents and strengthen resilience. Since its establishment in 2016, its mission has been clear: to make the UK the safest place to live and work online. The NCSC continues to deliver against that mission today.

New technologies are creating extraordinary opportunities for growth, innovation and prosperity. But they are also reshaping the cyber threat landscape. Artificial intelligence is accelerating change, increasing the scale and speed at which cyber threats can emerge, and exposing weaknesses in the technologies and systems we rely upon every day.



> ‘The response is not to fear technological change, but to adapt to it.’



Across GCHQ and the NCSC, we are developing new approaches to cyber defence, including pioneering work on Cyber Shield and the responsible application of AI to strengthen the UK's cyber resilience.

But technology alone will not solve this challenge. We need every organisation in the UK to take action now. Not only to protect their customers, services and livelihoods, but because cyber security is now part of the frontline defence of our nation.

Looking at Russia alone, it is clear that cyber operations are increasingly integrated into conflict, and that tactics developed against Ukraine are now being directed more widely against states and their institutions.

We cannot know what the next decade will bring, but we do know we must be ready.

That means modernising technology and building resilience at the pace demanded by a rapidly changing world. It means moving from understanding cyber risk to reducing it. And it means preparing for disruption, ensuring essential services can be maintained, recovery can happen quickly, and organisations can operate with confidence during periods of heightened threat.

These are no longer optional choices. They are fundamental requirements of a secure and resilient society.

None of us can meet this challenge alone, but together we are greater than the sum of our parts. The NCSC's success over the past decade has been built on partnership, and its future will be too. I'm immensely proud of the entire NCSC team for their work protecting our national security, our economy and our way of life.

Anne Keast-Butler,
Director GCHQ

A vision for the future

Imagine.

A nation where cyber security is not simply a technical discipline, but a strategic advantage.

A secure digital society.

A cyber-literate nation.

A thriving cyber economy.

A country strengthened by deep partnerships with allies around the world.

Not because cyber threats have disappeared. They will not.

Not because technology has stopped advancing. It will not.

But because we chose to build security, resilience and trust into the foundations of modern life.

We see a future where security is built in, not bolted on.

Where resilience is embedded across government, critical infrastructure, business and the wider economy.

Where organisations big and small can protect themselves, recover rapidly and continue delivering for the people who rely on them.

Where every organisation understands that cyber resilience is not just an IT issue, but a leadership responsibility.

Let's build a future where cyber attacks no longer have the power to significantly disrupt businesses, public services and citizens' lives.

Where secure-by-design technology becomes a source of competitive advantage.

Where world leading research drives world leading businesses.

Where security enables growth, innovation and prosperity.

And where the UK works with our allies to strengthen collective resilience and together shape a more secure digital future.

Just as previous generations built the roads, railways and energy networks that powered Britain's success, our generation must build the digital foundations on which our future prosperity will depend.

Because ultimately, this vision is not about cyber security alone.

It is about what cyber security makes possible.

A stronger economy.

Better public services.

Greater national security.

That is our vision.

Not simply a safer and more secure United Kingdom.

A more resilient one.

A more competitive one.

A more prosperous one.

A nation that sets the standard for what a trusted digital society can be.



UNDERSTANDING THE THREAT

The threat picture of the last 10 years is a story of both remarkable continuity and change.





Continuity and change

A decade of cyber threat

Technology has changed dramatically over the last decade, but many of the weaknesses exploited by attackers are remarkably familiar.

It's been another year of destructive cyber attacks, with the familiar story of state-sponsored espionage and cyber crime conducted at scale.

Russian hacking groups engage in offensive cyber operations in Ukraine, including disrupting power generation. Critical infrastructure and government institutions continue to be targeted by state actors, including a massive breach of government personnel records. Meanwhile, UK telecoms and health sectors are victims of high-profile ransomware attacks in pursuit of financial gain.

Except the year in question is not 2026. It's 2015, and the incidents described above are - respectively - the Sandworm power grid attacks, the US Office of Personnel Management breach, the TalkTalk data breach and attacks on US hospitals by Russian-based ransomware groups.



Those incidents from ten years ago tell us something important about the cyber threat. While technology has changed dramatically over the last decade, many of the weaknesses exploited by attackers remain remarkably familiar. The threat picture of the last ten years is therefore a story of both remarkable *continuity* and *change*. Understanding both is vital to give us a clearer view of the challenges ahead, and also warns us of the consequences of complacency.

There's continuity in the actors we face and the tools they use. The most serious adversaries we face today are the same as they were a decade ago. Their core tactics have evolved, but their success still relies extensively on the targeted exploitation of the scaled and known vulnerabilities across government, economy and society. The bulk of capability we have seen deployed in recent state-backed incidents is not an advanced, autonomous end-to-end AI attack, but a much simpler exploitation of common vulnerabilities and exposures (CVEs) and other open vulnerabilities, based on a decade of operational experience, patience and understanding of what works.

> 'There's continuity in the actors we face and the tools they use. The most serious adversaries we face today are the same as they were a decade ago.'

In other words, the same well-established attack techniques continue to deliver results for attackers. Our data from the incidents we handle supports this. For large organisations, 88% of incidents came from four initial access vectors:

- exploiting external public-facing applications
- phishing
- misuse of valid accounts
- exploiting external remote services

But change is here as well. Autonomous end-to-end AI capability is coming into view. Threat actors are using and experimenting with AI across the full threat stack. We increasingly see the effects of automation in driving scale, efficiency and effectiveness, and the potential to outpace defences.

What once required significant time, effort and expertise can increasingly be achieved faster, more cheaply and by a wider range of actors.

At the same time, the 'widening gap' we highlighted in 2024 is growing. Organisations that modernise their technologies, address vulnerabilities and strengthen resilience are becoming more secure. Those that do not are finding it harder to keep pace with an evolving threat, as evidenced by recent attacks on programmable logic controllers (PLCs).

These attacks come at a time when the number of adversaries, state and non-state, continue to grow. Driving all of these developments is a world that's far more confrontational than in 2015, in which cyber capabilities are now an increasingly important component of national power.

The lesson is clear. We must learn to live with both continuity and change. Both long-term relatively static threats and emergent new threats. We need to prepare now for the large-scale exploitation of vulnerabilities and weaknesses that attackers continue to target every day. At the same time, we must prepare for the impact AI will have on the speed, scale and effectiveness of cyber operations.

AI, decades in the making, represents both continuity and change. Today, in the hands of threat actors, it is helping to industrialise many of the cyber attacks we have lived with for the past decade, allowing them to identify vulnerabilities, target victims and operate more efficiently. Looking further ahead, AI has the potential to become a genuinely novel cyber capability, enabling new forms of attack and fundamentally changing cyber security.

The threat development of the last decade reinforces a lesson from history; the more things change, the more they stay the same. If we have lived with broadly similar cyber attacks for the last decade, then we can say that our resilience has not yet been overwhelmed. We cannot spend our time obsessing about the latest AI-driven threat, but equally we can no longer remain complacent.

History shows us a way forward. The partnerships, interventions and innovations of the last decade have shown that progress is possible. The future will depend on whether we can scale those efforts quickly enough to keep pace with a changing threat.

The cyber threat to the UK

A more contested, competitive and technologically accelerated cyber environment.

Cyber attacks are no longer just a means of stealing secrets or disrupting systems. They are increasingly a tool used to shape economic outcomes, project state power and pursue strategic advantage. We've identified four interconnected trends, summarised below, to help understand the cyber challenge facing the UK today.

1. China is changing the scale of cyber competition

China's adversarial cyber activity represents the most sophisticated and sustained cyber challenge facing the UK.



China's rapid development into a tech superpower is distinguished by its scale and its 'whole-of-state' approach, which sees it combine legislation, private sector contractors and technology development to achieve its goals.

Data sits at the centre of China's approach, and in this AI era, data is more valuable than ever. China uses its advanced cyber capabilities to acquire large amounts of information from the UK and elsewhere. It trains models, improves capability and generates insight. China's ability to acquire, process and exploit vast quantities of information

therefore has implications far beyond traditional espionage.

Its growing influence in global technology markets and standards further strengthens its ability to project cyber power internationally.

China Case Study: Use of compromised devices to conduct cyber espionage

In December 2025, the UK government sanctioned two technology companies based in China for their reckless and indiscriminate malicious cyber activity against the UK and its allies.

- **Sichuan Anxun Information Technology co Ltd**, known as i-Soon, targeted over 80 government and private industry IT systems across the world and supported others to carry out malicious cyber activity.
- **Integrity Technology Group** ran a covert network and provided technical assistance to enable further attacks. This company was also **assessed by the FBI** to be responsible for the computer intrusion activities attributed to China-based hackers known as Flax Typhoon.

In April 2026 the NCSC, alongside 15 international partners from across nine other countries, **issued a joint advisory**, highlighting how to defend against these attacker tactics which are believed to be used by the majority of China-linked actors to disguise malicious cyber activity.

2. Cyber operations have become a tool of state power

Cyber operations are increasingly being used alongside diplomacy, economic pressure, military power and information operations. Nation states use cyber capabilities to enable espionage and interference operations (such as hack and leak or transnational oppression), planning of lethal operations, acquisition of sensitive economic data, and operations to disrupt or destroy assets and services.

The growth of the commercial cyber intrusion marketplace has almost certainly lowered the barrier to entry for states to acquire commercial cyber intrusion capabilities (CCICs), enabling a broader range of actors to conduct sophisticated cyber operations.

During periods of heightened tension or crisis, the cyber threat to the UK can escalate rapidly and without warning. Cyber vulnerabilities can quickly cascade into loss of individual, business or government data and lead to societal harms.

While the threat will change in line with intent, Russia currently represents the most audacious cyber threat to the UK. Elsewhere, Iran-linked groups continue to demonstrate how cyber operations can be used to create indiscriminate disruption at scale.

Russia Case Study: Exploiting vulnerable routers to target critical national infrastructure

In July 2026 the NCSC, alongside 18 international partners from across 12 countries, **issued a joint advisory**, highlighting the methods of Federal Security Service (FSB) Centre 16 cyber actors. They were exploiting vulnerable routers and globally targeting networks belonging to critical national infrastructure (CNI). On the same day, **the UK government sanctioned 24 individuals and entities** behind destructive cyber and hybrid operations including cyber criminals involved in proxy networks linked to the Russian Intelligence Services. The UK and EU member states formally attributed an attack on Poland's energy grid in December 2025 to Russia's FSB Centre 16. The attack, if it had been successful, could have caused 500,000 citizens to lose electricity.

3. Economic security depends on cyber security

Cyber threats are increasingly translating into real economic harm in the UK. Ransomware, data breaches and supply chain compromises disrupt business operations, halt production and impose significant recovery costs.

Cyber espionage is highly likely to be the most significant cyber threat to the UK's long-term economic growth. The financial consequences accumulate through reduced innovation, diminished competitive advantage and lost commercial opportunities, with high-value, knowledge-intensive sectors increasingly attractive targets for cyber espionage.

According to UK **government research**, malicious cyber activity costs UK organisations an estimated £14.7 billion every year. Put another way, cyber attacks are wiping out value equivalent to the size of the UK's cyber security sector annually.

Automotive Sector Case Study: Jaguar Land Rover cyber incident

The cyber attack that affected Jaguar Land Rover (JLR) in 2025 caused severe and prolonged disruption to its global production and retail activity, with significant impacts across the supply chain. As one of the UK's largest automotive manufacturers, the effects extended beyond JLR itself, impacting suppliers, retail operations and wider economic activity linked to the UK automotive sector.

Suppliers reliant on JLR's production schedules, orders and payment processes experienced operational challenges and workforce pressures as the effects of the incident were felt. JLR reported approximately £196 million in direct cyber-related costs. The attack had a direct impact on GDP, contributing to the UK economy expanding by only 0.1% in Q3 2025 (lower than originally forecast).

4. Technology advances are changing and increasing the threat

Technology has always influenced cyber security. What is different today is the pace. The ability of state actors to harness new technologies will increasingly determine their effectiveness.

AI, automation and advances in computing power are already helping some threat actors identify vulnerabilities, target victims and operate more efficiently.

By 2028, it is highly likely China, Russia, and other nation states will routinely use AI cyber to achieve their geopolitical goals with the UK facing an increase in scale and speed of sophisticated cyber attacks.

It is also highly likely that between now and 2028, AI-powered malware will have been used in a ransomware attack on UK CNI.

In addition, increased reliance on space-based technologies will also expand the threat surface, providing more opportunities to adversaries over the next ten years.

Responding to these challenges

These four trends point to a clear challenge: the UK is operating in a more contested, competitive and technologically accelerated cyber environment. The answer is not to choose between today's threats and tomorrow's. We must address both.

The vulnerabilities that attackers exploit today remain well understood, while new technologies are increasing the speed and scale at which they can be exploited. The challenge for the UK is therefore straightforward: strengthen resilience now while preparing for what comes next.

Defending Democracy Case Study: Targeting of election candidates and democratic institutions

Hostile states continue to target election candidates, elected officials and democratic institutions in attempts to gain access to sensitive political and government information. During the year, the NCSC observed persistent spear-phishing activity against high-risk individuals and increasing efforts to compromise messaging applications.

The NCSC responded by updating guidance relating to a Russia-linked threat actor known for spear-phishing campaigns and expanding its **high-risk individuals guidance** to include securing messaging applications. During a year that included local elections, Scottish Parliamentary and Senedd elections, by-elections and a transition to a new Prime Minister, the NCSC worked closely with the Joint Election Security Preparedness Unit, political parties and other democratic institutions to help strengthen the resilience of the UK's democratic processes.



The impact of AI on cyber threat

Artificial intelligence is already beginning to reshape the cyber threat landscape. While AI is unlikely to fundamentally change the goals of hostile actors, it is highly likely to increase the speed, scale and efficiency with which they operate.

The following assessment sets out the NCSC's key judgements on how AI is expected to affect cyber security.

It is almost certain AI will act as a force multiplier across the cyber threat landscape, allowing skilled threat actors to carry out operational tasking at increasing scale, speed and efficiency.



The latest advancements in AI models are transforming cyber operations by enhancing multiple stages of the attack lifecycle, including reconnaissance, social engineering, vulnerability discovery, and coding for exploit development. Despite this, the adoption of AI among threat actors remains uneven. It is almost certain that AI presents a challenge for the UK around how to best defend and remain resilient from AI-assisted operations emanating from state, state-aligned and non-state actors. The greatest impact of AI will be the acceleration and scaling of existing tactics, techniques and procedures (TTPs) as opposed to generating new attack vectors.

It is highly likely AI will continue to be integrated into threat actors' cyber operations, increasing the speed, scale and efficiency of existing attack methodologies rather than autonomously conducting end-to-end attacks.

Human operators highly likely remain essential for directing, validating and adapting AI-generated outputs with human-machine teaming required for cyber operations. The uplift AI provides remains uneven across the attack lifecycle, with skilled operators seeing the greatest benefit, allowing them to streamline existing operational workflows and to focus on tasks where AI is less proficient. The higher the skill of the operator directing the model, the greater the efficiency gains and success rate. Loss of control whilst running an agentic AI will highly likely hinder threat actors from achieving their intended objectives, underscoring the need for effective human oversight during operations.

It is highly likely the use of AI-assisted vulnerability discovery and exploit development will pose a significant threat, giving threat actors a greater opportunity to target systems before they are patched by system owners.

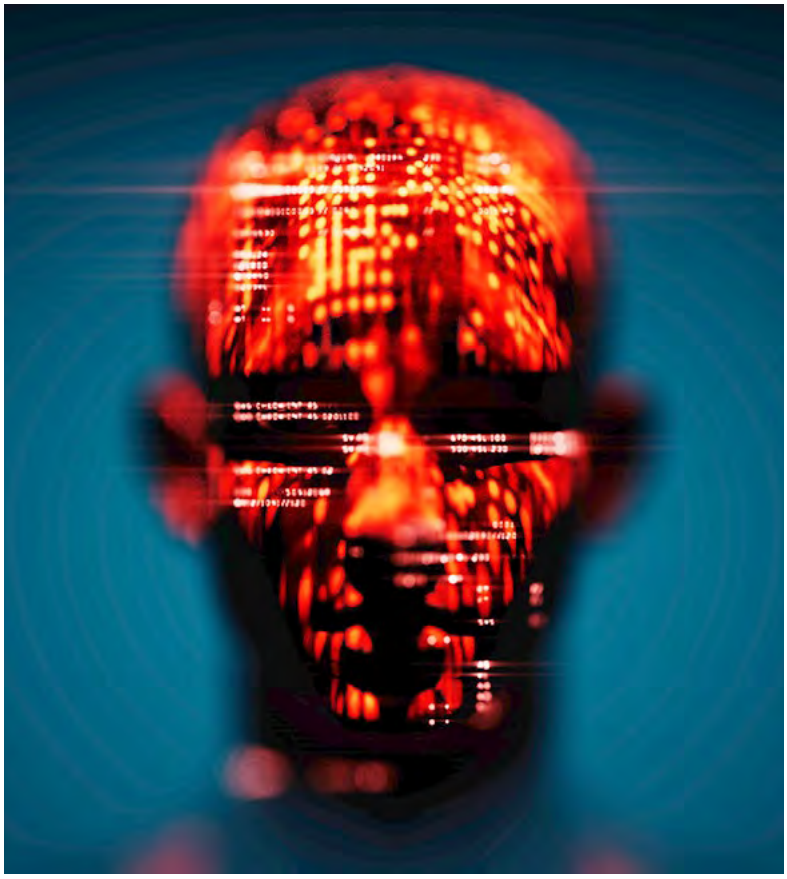
AI models have become capable of detecting vulnerabilities in large codebases and misconfigurations in systems that have historically remained undetected.

Not all vulnerabilities discovered by AI models will pose an immediate threat or be exploitable. However, it is highly likely defenders and maintainers of systems will face a race to shorten patch deployment timelines to mitigate against the influx of vulnerabilities before threat actors are able to develop any working exploits against them.

It is almost certain a widening digital divide will emerge between organisations able to adopt AI for defence and those unable to adapt.

The cyber security benefits of AI will not be distributed evenly. Organisations with mature cyber security programmes, sufficient resources and robust AI governance are likely to improve their ability to detect threats, prioritise vulnerabilities and automate defensive processes. Organisations with weaker security postures, legacy technology and limited resources may struggle to keep pace with the increasing speed of AI-assisted attacks. This divergence is likely to create a widening gap between resilient and vulnerable organisations, with the latter becoming increasingly attractive targets for both state and criminal actors.

China highly likely has the intent and is best positioned to use AI for operations against critical national infrastructure and other strategic targets.



While other states will also benefit from AI-assisted cyber capabilities, China's investment in AI and its ambition to become a leading science and technology superpower means it is highly likely to benefit from AI enhanced operations. The development of its own frontier AI capability programmes will almost certainly allow China to improve the identification of vulnerabilities, increase targeting efficiency and enhance access operations against critical national infrastructure and other strategic targets.

It is highly likely the use of 'shadow AI' will leave the cyber security of an organisation open to exploitation from advanced persistent threat groups and cyber criminals.

Employees transferring sensitive company or proprietary data onto their personal devices to use shadow AI almost certainly means organisations will lose visibility of how the information is handled and who can access it. It is also likely organisations will lose sight of their workforce's competency in cyber security if the tasks are frequently outsourced to shadow AI. This will likely increase an organisation's vulnerability to attackers.

It is highly likely AI malware will be used in a ransomware attack on UK CNI.

Cyber criminal adoption of AI will highly likely increase the scale and efficiency of ransomware operations, social engineering and vulnerability exploitation. Open source AI tools originally intended to assist security researchers are likely to be repurposed by cyber criminals to orchestrate and automate their existing workflows. This is expected to further reduce operational costs for criminals while increasing attack volumes against less resilient targets.

The age of autonomous attack

We can build a more secure, resilient and prosperous digital future, where the UK benefits from technological change while managing its risks. But that future is not guaranteed. The following pessimistic scenario explores one plausible future in which resilience improvements fail to keep pace with technological change and hostile actors exploit AI at scale. AI-cyber capability proliferation far outstrips UK's defensive ability. The purpose of this scenario is not to predict the future, but to illustrate the consequences of inaction and highlight the importance of the choices we make today.

Scenario: AI-cyber capability proliferation far outstrips UK's defensive ability

In 2028, the widespread availability of frontier AI capability to all from state level threat actors to independent novice hackers has led to a significant increase in the frequency and sophistication of cyber attacks worldwide. The UK faces a significant increase in cyber attacks targeting its CNI, industry, government, and civil society.

The proliferation of advanced AI-cyber capability has made it increasingly difficult to attribute attacks to specific threat actors. China, as a leading developer of AI-cyber capability, has likely played a role in disseminating advanced capability to

other actors, enabling them to hide their activities within the noise. The use of proxies has become more common, further complicating attribution efforts.

A new threat has emerged in the form of an automated cyber actor, utilising frontier AI, which is no longer under its operator's control. It is a realistic possibility such an entity could self-replicate and conduct cyber attacks at will,



with no apparent motivation or restraint. The lack of intentionality of such an actor and the multiple parties affected by such activity would likely complicate geopolitical issues. This would also likely make intentional harm caused by adversaries more deniable.

The situation is further complicated by the increased commercial availability of AI tools, including jailbroken models, in the criminal marketplace. This has widened the availability of advanced AI-cyber capability beyond sophisticated actors to include inexperienced cyber actors, such as novice or amateur non-professionals, who may not fully understand the risks and consequences of their actions.

In 2028, there is more potential for AI to coordinate cyber compromise impacting the physical world due to the increased cyber-physical interface with more AI controlled robots, cloud controlled CNI and greater integration of cyber into physical (e.g. biological) labs.

The increased activity from non-state actors and immature threat actors has likely intensified geopolitical tensions, particularly where they are perceived to be emanating from a specific country or region. Espionage activity has also likely increased, with AI-enabled espionage capabilities making it easier for threat actors to remain undetected.

The UK's use of AI-cyber security tools for defensive purposes has helped to mitigate some of the threats, but it is unclear whether this will be enough to counter the rapidly evolving threat landscape. The situation is likely to be worse than currently known, with many variables and unknowns still to be discovered.

Incident management

The NCSC Incident Management Team (IM) responds to cyber incidents affecting UK organisations. It plays a central role in triaging reports, supporting affected organisations, and coordinating NCSC and cross-government responses to nationally significant incidents, helping to ensure that the risks they pose to the UK are managed effectively.

This year, the IM team received 1,831 reports of cyber attacks affecting organisations across a range of sectors. Following triage, 337 incidents required support from the team, of which 80 were classed as nationally significant. In addition, through the NCSC's Early Warning service, IM notified 8,500 organisations of events that indicated a suspected compromise of their systems. Rapid notification via automated systems of early stages of attacks helps organisations deal with minor incidents before they can grow into ones that require NCSC support.

It is important to note that incident reporting does not follow a simple year-on-year trend. There is never a flat trend in incident activity, and peaks in previous years have often been associated with a small number of particularly significant incidents. Equally, the impact of proactive measures should not be overlooked.

The scale of notifications generated by the Early Warning service is likely to have headed off a number of incidents before they developed into events requiring NCSC intervention.

These figures do not tell the whole story: the scale and complexity of incident response vary greatly. Several high-profile incidents during the year required support from across the NCSC, including invaluable assistance from the Legal and Media teams.

Most successful compromises still rely on familiar methods. Threat actors routinely exploited known vulnerabilities in internet-facing systems, used stolen credentials, and employed social engineering to gain access to networks. Fundamental security measures therefore remain critical to organisational resilience, including wider adoption of passkeys in place of passwords to reduce the risks associated with stolen credentials.

The year included a number of incidents assessed as having links to state or state-aligned actors. Although their objectives often differ from those of cyber criminals, many target vulnerabilities in internet-facing systems. While some cases involved exploitation of previously unknown vulnerabilities, many involve vulnerabilities for which patches are available but have not been deployed in a sufficiently timely fashion.



Organisations are increasingly reliant on suppliers, service providers and other trusted third parties to deliver critical functions, and weaknesses or compromises within a supply chain can expose them to risks beyond their immediate control. Understanding these dependencies and engaging suppliers on cyber security are therefore important elements of managing cyber risk. The government's Cyber Resilience Pledge includes a commitment to roll out Cyber Essentials across supply chains for this reason.

The IM team has also begun to see threat actors incorporating AI tools into their attacks. None of the observed uses of AI enabled a novel class of attack, reinforcing the importance of consistently applying established security controls.

The cyber threat to the UK's Critical National Infrastructure (CNI) also remains enduring. The NCSC continued to observe activity affecting CNI and its supporting ecosystem, including activity believed to be linked to nation states. Such activity may be intended to gather intelligence, gain access to sensitive networks, or establish a foothold in systems of strategic interest. In addition, the Government Cyber Coordination Centre (GC3, a joint initiative between NCSC and the Government Cyber Unit) has seen activity targeting government.

Potentially increasing exploitation of vulnerabilities affecting internet-facing systems within CNI environments reinforces a familiar lesson from incident response activity: even sophisticated adversaries frequently gain initial access through known and often preventable weaknesses. This underlines the importance of maintaining strong cyber resilience across the UK's essential services.

The incidents handled by the NCSC this year reinforce a clear message: the cyber threat to the UK remains significant, with most successful attacks still exploiting familiar weaknesses. Strong cyber hygiene, informed and vigilant staff, effective monitoring and incident response, and resilient supply chains remain among the most effective ways to reduce cyber risk and limit the impact of incidents.

7 things we learned

What 337 incidents revealed about cyber resilience in the UK.



1. Attackers exploit the basics

- known vulnerabilities
- poorly secured systems
- internet-facing assets remain a primary route to compromise



2. People remain a target

- social engineering
- credential theft
- security culture matters



3. State and criminal actors share weaknesses

- similar routes to compromise
- vulnerability exploitation
- credential abuse
- poor cyber hygiene creates opportunities for all threat actors



4. Ransomware remains highly disruptive

- extortion
- data theft
- operational disruption
- long recovery timelines



5. Preparation determines outcomes

- logging
- monitoring
- incident response planning
- supply chain resilience



6. Early action reduces impact

- Early Warning notifications
- faster detection
- containment before escalation
- incidents prevented from requiring NCSC support



7. Sophisticated actors don't have to be sophisticated to gain access

- initial access doesn't have to be sophisticated
- onward activity by the actor is where sophistication becomes evident



Key Takeaway: Most successful attacks continue to exploit familiar weaknesses. Improving cyber resilience fundamentals remains the most effective way to reduce both the likelihood and impact of cyber incidents.



TECHNOLOGY AND THE FUTURE OF CYBER SECURITY

The defining cyber security challenge of the next decade is adapting quickly enough to keep pace with AI.



A decade of technological change

The next 10 years will be defined by increasingly capable AI systems and machine-speed cyber operations. Understanding these shifts is critical to maintaining the UK's cyber resilience.

When the NCSC was established in 2016, many organisations still thought about cyber security in terms of the networks they owned, the data centres they operated and a perimeter they could defend.

Since then, hyperscale cloud, software as a service and ubiquitous connectivity has redrawn the terrain. Our cyber security approach has moved towards zero trust approaches based on strong identity, explicit verification, attestation and least privilege. The COVID-19 pandemic compressed years of digital transformation into months, accelerating remote working and our reliance on collaboration platforms.

> Organisations need to understand what data a model can access, what tools an agent can invoke, what instructions it trusts and how its actions are observed and constrained.'

These changes delivered substantial benefits. Cloud providers could deploy a security improvement once and protect millions of users, and empower organisations with sophisticated capabilities they could neither build nor sustain themselves. But it also left many organisations managing increasingly

complex technology estates, legacy systems and accumulated technical debt. AI is now exposing many of those weaknesses at machine speed.

The next phase is not simply 'more digitalisation'. It is the development and exploitation of systems that generate, reason, plan and



increasingly act with autonomy. Cloud infrastructure allows the centralisation and utilisation of data and compute at scale. APIs make services composable, and software delivery continuous. These conditions allow AI capabilities to be integrated rapidly into products, business processes and services.

The democratisation of capability

Frontier AI systems mean tasks that once required specialist knowledge and skills can increasingly be accessed by a broader cross-section of individuals and organisations through smaller and cheaper and open models. The result is a democratisation of technological capabilities, with more people creating software, analysing data and automating tasks.

This democratisation has significant defensive potential. Organisations that previously lacked access to specialist cyber expertise can access sophisticated security capabilities, while skilled cyber security professionals can automate routine analysis and spend more time on judgement, research and the hardest problems.

But democratisation also enables malicious use, helping less capable attackers to adapt or produce malware, and automate the exploitation of vulnerabilities. Agentic systems can be given an objective, select tools, sequence actions, inspect results and adapt their approach with varying degrees of human oversight. The consequence is not new categories of cyber risk, but rather the sharp increase in the speed, scale and persistence of familiar risks.

In cyber security, this matters because security controls have traditionally been built around human limitations. Security experts work at human speed, require rest, cannot inspect every event and operate within social and organisational constraints. Agents can run continuously, operate multiple tasks and act across many systems at once.

A moderately capable system operating at scale can therefore be consequential, even without making wider conceptual leaps traditionally associated with expert-led cyber security development.

Over time, the same capability will support a correction. Technology vendors will use AI throughout the development lifecycle to identify flaws before release, generate and test fixes, and protect customers of managed services. Defenders will use agents to discover network vulnerability, triage alerts, map networks and rehearse response. The structural advantage will remain with defenders; they own or operate the environment, can instrument it, can change it and can define acceptable behaviour. But this advantage is not a given, and realising it requires clear direction, investment and disciplined adoption.

Equally important is ensuring organisations *develop* AI systems securely, whether those systems have been created from scratch or built on top of tools and services.



As our **world-leading guidance on secure AI development points out**, organisations need to understand what data a model can access, what tools an agent can invoke, what instructions it trusts and how its actions are observed and constrained. This means security must be considered across the whole AI lifecycle: design, development, deployment, operation and maintenance.

The consequences of compromise in the *physical* world

As AI becomes embedded in connected devices that sense and act in the physical world - think robotics, autonomous vehicles, drones, connected medical devices and industrial systems - the consequences of compromise will also change. Where systems interface with the physical world, security priorities must include safety, reliability, availability and resilience, not just information protection. Cyber security increasingly becomes a *societal* issue rather than a purely *technical* one, as the attack surface expands to include *trust* in information, institutions and digital interactions, creating new challenges around fraud, misinformation and authentication.

An approach based on discovering and manually patching every flaw cannot



keep pace with machine-speed vulnerability discovery. Automated remediation will be part of the answer, but automation applied to insecure foundations does not address the fundamental issues. The longer-term goal must be technology that *prevents broad classes of vulnerability*, and limits the consequence of those that remain.

This requires investment across the technology stack. Secure development practices can make vulnerability prevention part of normal engineering. Hardware-backed security, strong identity and trustworthy update mechanisms can provide dependable control points. This connects to the NCSC's work on cross domain technologies: as AI, cloud, operational technology and higher-assurance environments become more interconnected, we will need ways to move data and insight safely between differing trust domains.

The long-term goal is technology that is secure by design and resilient by default. But while these technological shifts gather pace, organisations must still take practical action to reduce risk today. The challenge for the next decade is combining stronger foundations with consistent implementation of proven cyber security practices. The **NCSC's Principles Based Assurance** will help with this, moving assurance away from static compliance gained from a one-off assessment, towards confidence in security *outcomes*. It asks whether a product, system or service can make credible security claims, support those claims with evidence, and maintain that confidence as technology and threats change. That approach matters even more as AI accelerates vulnerability discovery and increases the pressure on organisations to patch and respond quickly.



Roles and skills will also change. AI can raise the productivity of experienced practitioners by allowing multiple lines of analysis, and a more strategic focus of effort. It can help those new to cyber security learn and broaden participation. However, if entry-level tasks are automated without redesigning training pathways, the profession may inadvertently weaken the pathways through which people acquire deep expertise. Organisations should preserve deliberate practice, mentoring and opportunities to work through problems rather than only review machine-generated answers.

From research to real-world impact

Over the past decade the UK has built one of the world's most respected cyber security research ecosystems, bringing together government, academia and industry to address some of the hardest cyber security and technology challenges we face. This ecosystem has consistently delivered advances that improve our national security while also supporting economic growth, innovation and broader skills development.

At the heart of the NCSC's technical capability are our own experts, who combine operational experience with long-term research and technology leadership. Their work helps identify emerging risks, shape standards, influence global technology development and ensure that security considerations are built into new technologies from the outset.

Research matters because it delivers practical outcomes. Examples such as **SilentGlass** - a device that blocks anything unexpected or malicious between HDMI and Display Port connections and screens - demonstrate how long-term investment in cyber security research can translate into capabilities that directly improve national security and resilience.

Within the UK research community, the **NCSC Academic Centres of Excellence in Cyber Security Research (ACE-CSR)** network brings together universities

undertaking internationally recognised cyber security research across a wide range of disciplines, from secure systems and cryptography to human factors, artificial intelligence and cyber-physical resilience. Alongside this, the NCSC and UK Research and Innovation (UKRI) support a number of **Cyber Security Research Institutes (RIs)** that focus expertise on strategically important national challenges. Together these partnerships create a powerful national capability, provide pathways for new ideas to become deployable technologies, and help develop the next generation of cyber security professionals that the UK economy needs.

Preparing for the quantum transition

AI may dominate the immediate technology landscape, but it is not the only major transition. Over the past decade, our work on post-quantum cryptography (PQC) has ensured our most critical systems are resistant to the threat, and that we can provide world-leading guidance to help UK organisations migrate safely to PQC. We were the first major authority to set out publicly our early thinking on PQC, in a white paper published just 2 months after the NCSC was formed in 2016, and have produced influential guidance ever since.

In the past year, we have used our expertise to:

- support wider cross-government planning for PQC migration in partnership with the Government Cyber Unit
- contribute to international standards development
- raise awareness of the migration challenge in forums of industry leaders
- build PQC skills in the UK through our assured consultancy scheme
- lay the foundations for future regulation

2031 is a key date for the migration of critical services and components and the protection of high-priority information and services. Our role over the next few years goes beyond our history as cryptographers, to help move PQC into the cyber security mainstream.





BUILDING STRONG FOUNDATIONS

AI-assisted cyber attacks will ruthlessly expose organisations that don't have strong cyber security foundations in place.

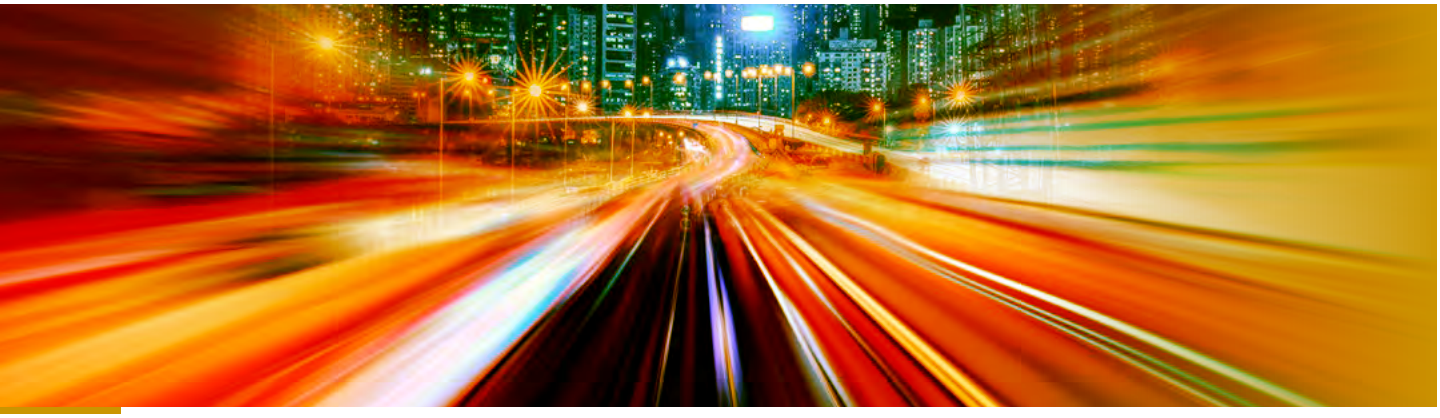


Embedding cyber security into everything

Building a resilient UK starts with embedding cyber security into technology, services, organisations, people and leadership. It also requires organisations of every size, from sole traders and small businesses to major employers and public sector bodies, to make cyber security part of their everyday business.

> ‘Success will increasingly depend on organisations’ ability to remediate, recover and adapt quickly, while using AI to strengthen cyber defence, identify threats earlier and improve resilience.’

The NCSC is helping organisations strengthen resilience through practical guidance, training, services and support. But the central message remains simple: cyber resilience needs to be built on strong foundations.





The good news is that we already know what works. Knowing what technology you rely on, keeping systems updated, controlling access to important accounts and information, backing up critical data and preparing for incidents remain the foundations of effective cyber defence. The challenge is no longer understanding what good cyber security looks like. It is putting it into practice, consistently, at scale and at the speed the threat now demands. For all organisations, this starts with implementing the five technical controls at the heart of Cyber Essentials: firewalls, secure configuration, security update management, user access control and malware protection.

Many successful cyber attacks still exploit weaknesses that are well understood and preventable. The NCSC continues to see the same vulnerabilities exploited time and again. These are vulnerabilities that are often straightforward for attackers to identify and for organisations to address.

This matters because AI is changing the economics of cyber attacks. It is making it easier to identify weaknesses, easier to target organisations and easier to operate at scale. AI did not create these weaknesses. It is exposing them faster than ever before. AI is increasing the urgency, but organisations still have a choice. Those that strengthen resilience, modernise ageing technology and address known weaknesses now will be better placed to manage risk and safely realise the benefits of AI.

AI does not fundamentally change what good cyber security looks like; it makes proven cyber security foundations more important than ever. Success will increasingly depend on organisations' ability to remediate, recover and adapt quickly, while using AI to strengthen cyber defence, identify threats earlier and improve resilience.

Ultimately, the organisations that invest in strong cyber foundations today will be the ones most capable of navigating future challenges and opportunities. In doing so, they will help build the trusted digital foundations on which the UK's future prosperity, security and growth depend.

Why ‘building strong foundations’ has never mattered more



Applying cyber security fundamentals is still the best way to repel many of the commodity attacks we see today.

When the NCSC was launched in 2016, Ciaran Martin – our first CEO – outlined **why the UK needed a National Cyber Security Centre**. His advice to CNI, SMEs and larger organisations was “Work out which bits are most relevant to you. Then focus on getting the basics right”.



Back then, ransomware attacks were still novel and artificial intelligence (AI) was a speculative issue for cyber security. 10 years later, cyber attacks by agentic AI tools can perform unsanctioned actions and can use ‘human-like deceptive behaviour’ on the open internet (what the media refer to as ‘**tech going rogue**’). But that original advice remains remarkably prescient, and it’s a consistent message that runs through all of the NCSC’s pages of guidance dedicated to **mitigating the threats from AI-assisted attacks**:



So what are 'strong foundations'?

A frequent complaint from business leaders (and everyday citizens) is that experts use complicated jargon when describing technology and cyber security.

Cyber security best practice. Maintaining cyber security fundamentals. Doing the basics. Strong cyber foundations. What good cyber security looks like.

These are all terms used by the industry to describe 'getting the basics right'. The reality is that without strong foundations in place, all organisations, regardless of size or sector they operate in, will be disrupted by cyber attacks. AI-powered cyber attacks are a force multiplier which makes it easier, faster and cheaper for an attacker to ruthlessly expose those organisations that don't have 'the basics' in place.

How do you build strong foundations?

For the last ten years, the NCSC has been developing a range of frameworks, tools, advice and guidance that will help you build strong foundations, whether you're a micro-business with a handful of devices to look after, or an SME with a growing IT estate to manage. These are summarised below, starting with the Cyber Action Toolkit for those who need help taking their first steps in cyber security.

The majority of cyber attacks rely on techniques that are well known, and that can be mitigated. Individuals and organisations that *implement* the NCSC's world-leading guidance, which can be downloaded and shared free of charge from our website, would be protected from such attacks. Organisations that do this also stand the best chance of repelling the next generation of AI-powered attacks.

> 'The best way to protect all systems, whether those threats are AI-assisted or not, is by making sure you have the cyber security foundations in place.'

The Cyber Action Toolkit

What is it, and who is it for?

The Cyber Action Toolkit is a free, web-based toolkit for sole traders and micro-organisations that you can access from your phone, tablet or computer. It turns the advice from the NCSC's experts into simple, achievable steps, with built-in features that recognise your progress.

How does it help me 'build strong foundations'?

The toolkit helps you to build layers of protection around your business. You'll start by protecting your most important accounts (such as your email and banking accounts) and learn how to protect accounts and devices by using password managers and passkeys or 2SV.

By the time you've completed the toolkit, you'll be able to spot cyber attacks, and to know how to recover your important data should the worse happen. You'll also have the foundations in place to work towards Cyber Essentials certification.

23,978 users have landed on the toolkit

14,200 steps have been marked as 'done'

The actions covered in the Cyber Action Toolkit

As you work through the toolkit, progressing from **Foundation** to **Improver** to **Enhanced**, you will build layers of protection around your organisation which defend against common cyber threats.

Foundation	Improver	Enhanced
Secure your business's email accounts	Remove unnecessary user accounts	Plan your response to a cyber attack
Use a password manager	Back up your important work files and data	Limit administrator access to cloud services
Secure your important online accounts	Create separate admin and user accounts on devices	Review your digital footprint
Check your devices are up to date	Learn how to spot a cyber attack	Consider Cyber Essentials
Update apps and remove unused ones	Check your antivirus and firewall	
Secure your devices		

1,761 accounts created

376 users completed Foundation, **247 Improver** & **188 Enhanced**

From action to certification: Supporting the journey to Cyber Essentials

Our ambition is for every UK organisation to get Cyber Essentials to reduce cyber risk and strengthen protection. To help organisations get there and meet the UK minimum standard for cyber security the NCSC provides a range of free support:

30 minutes of free support from a Cyber Advisor

Cyber Advisor is a network of cyber security consultants who've been assured by the NCSC to work specifically with smaller organisations. They understand how to apply the five steps that make up Cyber Essentials in a way that's practical, realistic and relevant for your business.

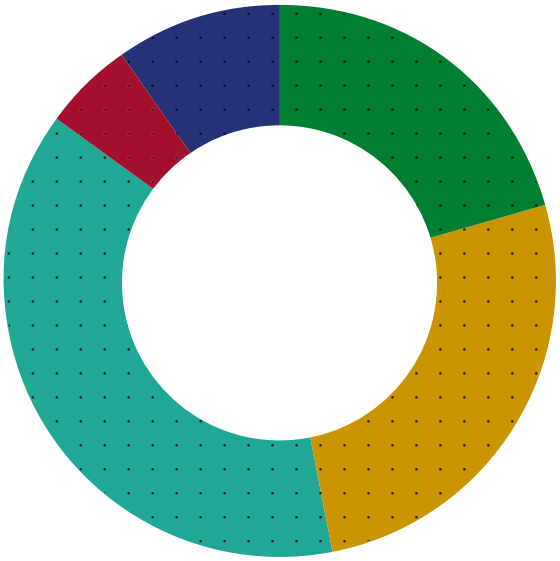
Since January 2026 around **1,235 requests** for free consultations have been made. Around **858** have been completed. (Aug 2026)

This has already led to over **256 small organisations** successfully gaining Cyber Essentials certification – which translates to a **30% conversion rate** – with many more under way.

The Cyber Essentials Readiness Tool

The Cyber Essentials Readiness Tool helps organisations understand how well they align with the Cyber Essentials requirements and provides tailored guidance on the steps needed to achieve certification.

The CE Readiness tool has been used **8,815 times** by organisations (August 2025 - September 2026).



Large	1,235
Medium	1,563
Small	2,250
Micro	3,112
Single person /sole trader	655

Top sectors using the CE Readiness tool, include: IT, Consultancy, Manufacturing, Charities, Construction, Health, Finance, Engineering, Managed Services, Academia, Legal, Retail.

Download the Assessment Questions

The free Question Set helps organisations understand the Cyber Essentials assessment questions, identify gaps and prepare for certification with greater confidence.

Downloads of the 'Question set': **31,408**

Downloads of 'Question set' and 'Requirements for IT Infrastructure': **51,424**

Cyber Essentials

What is it, and who is it for?

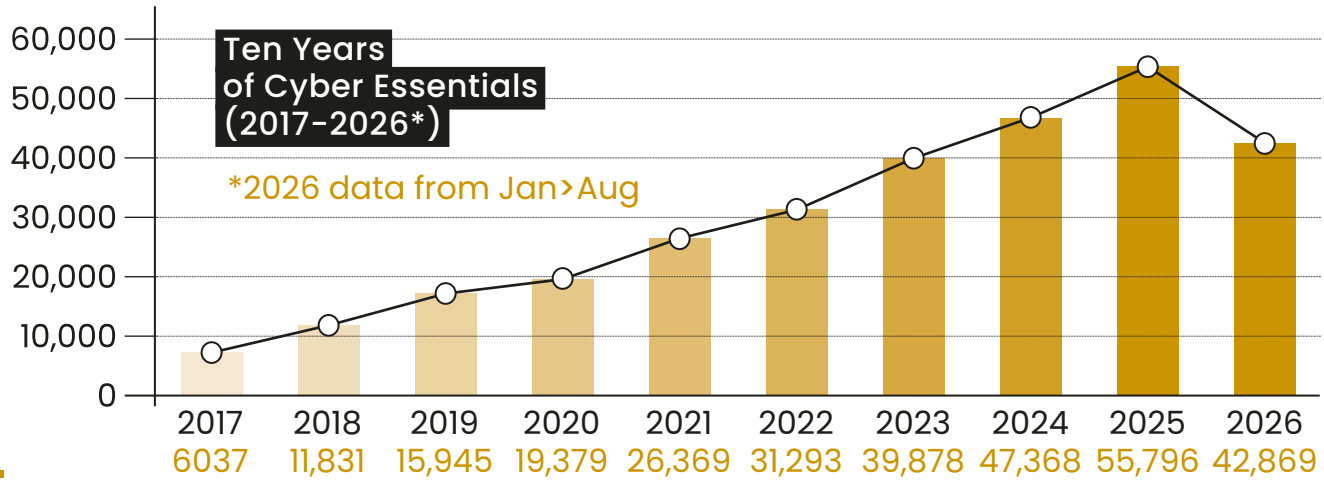
Cyber Essentials is the minimum standard of cyber security recommended by the government for UK organisations of all sizes.

Developed by the experts at the NCSC, the certification scheme is aligned to five technical controls designed to prevent the most common internet based cyber security threats. With Cyber Essentials in place, you'll have peace of mind that your organisation is protected against common online threats, and build customer trust as you've shown you take cyber security seriously.

How does it help me 'build strong foundations'?

Cyber Essentials helps organisations stay safe by ensuring **5 technical controls** are in place.

1. **Firewalls:** Create a security filter between the internet and your network.
2. **Secure configuration:** Set up computers securely to minimise ways that a cyber criminal can find a way in.
3. **Security update management:** Prevent cyber criminals using vulnerabilities they find in software as an access point to your systems.
4. **User access control:** Control who can access your data and services and what level of access they have.
5. **Malware protection:** Identify and immobilise viruses or other malicious software before it has a chance to cause harm.



Sept 25 > Aug 26

47,661 +19.6%
Cyber Essentials certifications awarded

15,646 +21.5%
Cyber Essentials Plus certifications awarded

444 +10.4%
Cyber Essentials Certification Bodies across the UK

Reducing Barriers to Cyber Essentials for SMEs

We know that organisations using Managed Service Providers (MSPs) can face additional complexity when working towards Cyber Essentials certification. To address this, the NCSC ran a pilot to explore the possibility of "badging" MSP's that can provide Cyber Essentials compatible services, with **28** providers taking part and **73%** meeting the required threshold. The pilot is informing a formal scheme, expected in 2026. This will help organisations identify providers who offer a service that will align with Cyber Essentials requirements and support wider adoption of the scheme across the UK.



Early Warning

What is it, and who is it for?
Early Warning is a free service available to any organisation within the UK. Once you've registered with the service, you'll be sent alerts that warn you of suspicious activity affecting your network.

How does it help me 'build strong foundations'?
Early Warning will notify organisations that have enrolled of any cyber attacks detected by our feed suppliers. It warns you about potential intrusions and vulnerabilities on your network, so you can act on them before they become bigger problems.

Early Warning delivers an average of 2,000 alerts each month to nearly 20,000 organisations, offering potentially invaluable time to detect and stop a cyber incident.

Early Warning numbers

19,922 organisations
signed up to Early Warning service.
A **52% increase** from last year

over 50 million
total events matched and sent in 12 month period

over 1 million assets
now signed up to Early Warning

Vulnerabilities:

we sent alerts to
232,777 unique IP addresses
with a vulnerability
— so if one IP got 50 alerts this would be counted as one

this breaks down to
11,558 unique organisations

Malware:

we sent alerts to
296,235 unique IP addresses
with a malware infection

this breaks down to
3,222 unique organisations

we alerted **1,018 unique organisations** to a compromised server in the reporting period. This was across
4,280 unique IP addresses

Securing the UK's internet

The NCSC works with internet service providers, hosting companies and cyber security partners to improve the underlying security of the internet, reducing opportunities for cyber criminals to operate and making the UK safer online. The NCSC's Active Cyber Defence programme has grown from a pioneering initiative into a national cyber resilience capability, helping organisations across the UK reduce exposure to common threats. It is a practical example of how the NCSC works with the wider ecosystem to raise security standards and strengthen resilience at scale.

Takedown

The NCSC's Takedown Service works with hosting providers to remove malicious websites from the internet - at scale and in near real time - and blocks any attack infrastructure to limit the harm that cyber criminals can cause. No registration is required for the Takedown Service. Central government organisations benefit automatically without having to sign up.

- **1.6 million+** cyber-enabled commodity campaigns disrupted
- **30,000** confirmed phishing attacks impersonating GOV.UK first taken down within a median of 90 minutes of detection
- Using our Takedown providers data (Netcraft), the UK share of global phishing was at its lowest **1.06%** in June 2026. This is the lowest it has been since the service started back in 2016 (previously over 5%)

Suspicious Email Reporting Service (SERS)

Since its inception in April 2020, the Suspicious Email Reporting Service (SERS) has enabled the public and businesses to report suspicious emails to the NCSC, leading to the removal of thousands of scams.

- **over 13.4 million** reports received in the 12 months (Sep 25-Aug 26 - the highest since the service started)
- total number of reports since April 2020 reached **over 58.9 million**
- **460,000 malicious URLs** removed by the NCSC since 2020

The NCSC Proactive Notifications Service

The NCSC:

- identifies organisations operating without essential security services
- sends these organisations emails to help them install software updates that can reduce vulnerabilities

This notification is based on scanning open source information, such as publicly available software versions. The service was launched to responsibly report vulnerabilities to system owners to help them protect their services.

More than 52,000 notifications have been sent, with 70% of the identified vulnerabilities subsequently resolved. Although some organisations may have remediated independently of the notification, the results and feedback indicate that the service is successfully identifying vulnerabilities and reaching affected organisations.

A recent trial found that organisations receiving notifications remediated identified vulnerabilities up to 45% faster than organisations that did not receive them.

Share and Defend

The NCSC works with the UK's Internet Service Providers to reduce the likelihood of individuals and organisations interacting with malicious content, criminal or otherwise. Developed by the NCSC, the Share and Defend service helps combat online crime by providing internet service providers with near real-time data on fraudulent and malicious websites. Providers can then use this information to prevent customers from accessing harmful sites, reducing the risk of cyber crime. This is one of the ways the NCSC works in partnership with businesses to strengthen the UK's cyber resilience and keep the public safe online.

Share and Defend protects over 61 million mobile subscribers and over 12 million fixed broadband subscribers across the UK from cyber-related harm, including cyber crime and cyber-enabled fraud. Since launch over one billion early-stage cyber attacks and attempts to access scam websites have been blocked.

Passkeys: Moving Beyond Passwords

The majority of cyber attacks against individuals begin with the theft, compromise or abuse of passwords. Even when combined with two-step verification, passwords and other authentication methods remain vulnerable to phishing and other common attack techniques.

Over the last year, the NCSC has promoted the adoption of passkeys as a safer, simpler and more resilient alternative to passwords. Passkeys replace passwords with cryptographic credentials that are



stored securely on users' devices. Because passkeys use public key cryptography and are tied to the legitimate service being accessed, they are significantly more resistant to the weaknesses that have plagued passwords for decades, including password reuse, weak passwords and phishing attacks.

In 2025, the **NCSC officially recommended passkeys** as the preferred authentication method for individuals. Since then, we've been working to accelerate passkey adoption at scale with technology providers and online services, and used CYBERUK 2026 to raise passkey awareness across industry, government and the wider public.

The UK is now recognised as a global leader in passkey adoption, with greater uptake with active Google users than in the US or the EU.

One of the most significant developments this year has been the introduction of passkeys to One Login, the identity service delivered by Government Digital Service (GDS) that enables citizens to access multiple services through a single account. The NCSC provided technical and security expertise to early adopters such as NHS England, the first government-sponsored app to offer *passkeys* as a login option for its service.

This represents a significant milestone in moving passkeys from a security concept to a technology that millions of citizens can use to access services more securely.

Although the NCSC is already working with other departments across government to support wider adoption, passkeys will only deliver their full security benefit if adoption extends *beyond government*, and becomes commonplace across the services people use every day. Over the coming year, the NCSC will continue working with technology vendors and service providers to encourage implementation and promote good practice. This will be supported by public communications activity designed to help citizens understand why passkeys are both safer and easier to use than traditional passwords.



SECURING THE BACKBONE OF SOCIETY

The resilience of the UK's most critical, complex and largest organisations will depend on decisions taken today.



A moment of choice

The challenge is no longer identifying risks to the UK's most critical organisations; it is acting on them.

Organisations facing the highest levels of threat, or whose disruption would have the most severe consequences, must take action now to prepare for the technological, operational and geopolitical challenges expected to shape the coming decade.

The emergence of frontier AI makes this challenge more urgent. As vulnerabilities become easier to identify and exploit at scale, organisations with ageing technology, limited visibility of their technology estates and slow remediation processes will find it harder to maintain resilience, particularly where they are subject to attacks and targeting by capable and well-resourced threat actors. At the same time, geopolitical instability means cyber operations are increasingly intertwined with national security, requiring organisations to prepare not only for today's threats, but for severe disruption during periods of heightened national tension.

The Cyber Security and Resilience Bill reflects the growing importance of cyber resilience to the UK's security, prosperity and public confidence.The measures set out in the Bill will introduce a more comprehensive, flexible and enforceable regulatory framework, with important new sectors brought into scope, new national security powers to respond to crises, and give government the agility to evolve the regulatory framework in a fast-moving threat



and technology landscape. Regulation can be one of the most powerful tools for driving sustained improvements in resilience at scale, but it alone will not deliver the outcomes we need. Organisations need clear expectations, regulators need effective ways to assess resilience, and leaders need confidence that critical services can withstand and recover from disruption.

This requires more than compliance. It requires organisations to understand the systems, technologies, suppliers and dependencies on which critical services rely, and to manage cyber security as a business risk rather than solely a technical issue. Boards and executive teams should seek assurance not only that policies exist, but that they can demonstrate measurable improvements in preparedness, recovery capability and resilience outcomes.

Government also has a unique responsibility. As one of the UK's largest and most complex technology enterprises, it must continue reducing technical debt, modernising critical systems and building resilience by design. By improving the resilience of its own systems and services, government can build trust, improve public confidence and demonstrate the effectiveness of good practice for the wider economy.

To support this, the NCSC is evolving its approach to cyber resilience. Alongside supporting implementation of the Cyber Security and Resilience Bill, we are improving the usability of the Cyber Assessment Framework (CAF), establishing more consistent resilience benchmarks and expanding assurance schemes that help organisations understand, measure and improve their resilience over time.

Government Cyber Action Plan: Delivering stronger cyber resilience across government

The Government Cyber Action Plan is transforming cyber resilience across government by setting clearer expectations, strengthening accountability and accelerating the adoption of shared capabilities.

This year, delivery through the plan has improved cyber risk management, expanded central cyber services and strengthened government's collective ability to identify, manage and respond to cyber risk. This includes the continued rollout of central cyber services, the growth of the Government Cyber Coordination Centre (GC3), and the establishment of the Government Cyber Profession.

One example of tangible impact is vulnerability management, which has helped reduce the median time taken to fix domain-related vulnerabilities from 50 days to 8 days, helping strengthen the resilience of systems and services relied on by citizens.

A minimum benchmark

The NCSC has recently published the CAF Core Profile, setting out our recommended minimum benchmark for cyber resilience for essential services and other organisations that are critical to the UK's security and prosperity. Informed by our assessment of the cyber threats facing the UK today, it provides a common baseline of resilience designed to mitigate risks from moderately sophisticated attackers. As a starting point rather than an end state, the profile provides a shared reference point for strengthening cyber resilience across the UK.

A clearer pathway to resilience

The NCSC is also developing a clearer resilience pathway for organisations seeking to build cyber maturity over time. This brings together the Cyber Action Toolkit, Cyber Essentials and the Cyber Assessment Framework as complementary stages, from foundational controls through to outcome-focused resilience management.

Providing confidence through assurance

Independent audit and testing are essential to prevent overconfidence in our defences and ensure that government, regulators and organisations themselves have a realistic picture of resilience. They also help organisations strengthen their cyber defences and demonstrate that they can withstand and recover from digital disruption.

Cyber Resilience Audit Scheme

The Cyber Resilience Audit Scheme enables trusted third parties to provide high-quality independent audits based on the CAF, boosting confidence in declared resilience levels. It is aimed primarily at operators overseen by regulators or other oversight bodies, but can also support any organisation seeking an independent assessment of its cyber resilience.

Cyber Adversary Simulation Scheme

Adversary simulation, sometimes referred to as red teaming, tests an organisation's ability to prevent, detect and respond to realistic cyber attacks. It is particularly suitable for organisations with mature cyber security processes and technical controls that want to understand how their defences would perform against a determined adversary.

Later this year, the NCSC will launch the Cyber Adversary Simulation (CyAS) Scheme as an MVP, providing assurance of suppliers delivering these services. The scheme , which has been developed in partnership with Cyber Oversight Bodies, is designed around realistic, reconnaissance-led testing and reflects how adversaries operate in practice, rather than relying on fixed or scripted approaches.

Beyond regulation

Even with stronger regulation, clearer benchmarks and improved assurance, resilience cannot be delivered through regulatory frameworks alone. Critical organisations must also be able to adapt quickly, learn from emerging threats and work together to strengthen collective resilience.

The NCSC increasingly focuses on building trusted communities of defenders, enabling organisations to share knowledge, expertise and operational experience. By bringing together organisations facing similar risks, these communities help strengthen collective defence and improve the UK's ability to respond to evolving threats.

Some risks, however, require more focused intervention. For a small number of the UK's most important critical systems, the NCSC is undertaking a multi-year programme of enhanced support designed to reduce risk and improve preparedness for severe cyber attacks, major disruption and periods of heightened national tension.

Supporting our most critical organisations

The resilience frameworks, benchmarks and assurance approaches described earlier are supported by a range of practical tools and services. Designed for critical, complex and nationally significant organisations, they strengthen cyber defences and demonstrate that they can withstand and recover from digital disruption.

Assured Cyber Security Consultancy

The NCSC's **Assured Cyber Security Consultancy scheme** helps organisations with complex, high-risk, or nationally significant cyber security needs identify trusted, independent consultancy providers. It provides assurance that participating consultancies meet our standard for delivering high-quality cyber security consultancy in accordance with the NCSC's advice and guidance.

Through the scheme, organisations can access expert support across a range of specialist areas including risk management, security architecture, and 'audit & review' services. Following updates to the scheme standard, including requirements for consultants to hold professional titles awarded by the UK Cyber Security Council, the scheme saw significant growth.

over the past year:
assured providers increased from
23 to 41 +78%

consultant numbers
increased from
59 to 90 +53%

CHECK Penetration Testing

Penetration testing is an effective way of finding vulnerabilities in your system before an attacker causes you harm. **CHECK** is the scheme under which the NCSC assures companies to conduct authorised penetration tests. It's been developed specifically for nationally significant organisations that face higher levels of threat.

Over the past 12 months, the NCSC's CHECK ecosystem completed approximately 3,000 penetration tests for more than 680 organisations across 40 sectors. In addition to helping organisations identify vulnerabilities, aggregated findings help increase the visibility of vulnerabilities, and identify common areas of exposure across sectors.

Cyber Resilience Test Facilities

The NCSC's new **Cyber Resilience Test Facilities (CRTFs)**, is a national network of assured facilities to help technology vendors demonstrate the cyber resilience of their products, and some services.

We established CRTFs to help consumers of technology to better

understand the cyber security of the products they are procuring. We'd encourage all technology vendors to use the CRTFs to provide confidence in their products. This confidence can, in turn, be shared to end users and customers.

This year marked an important milestone for CRTF, with the first products successfully assessed against NCSC-approved standards and methodologies. Since launching at CYBERUK 2025, the network has expanded to six facilities. CRTFs provide customers with meaningful, risk-based information about product resilience, helping organisations make more informed decisions about the technologies they deploy to support critical services.

Cyber Essentials Pathways

We know that many large organisations want Cyber Essentials Plus certification, but the way they operate does not always align with the technical controls required. Complex architectures, legacy systems, and layered security requirements mean that a purely prescriptive approach can sometimes feel more like a constraint than something that enables better security outcomes.

Cyber Essentials Pathways was designed to respond to this challenge, providing a way for organisations to demonstrate that their controls deliver equivalent (or better) protection, even where they differ from the standard Cyber Essentials model. Essentially, Pathways introduces flexibility without weakening the scheme's rigour. Cyber Essentials Pathways is all about giving organisations more than one way to demonstrate that they are achieving the same overall outcome. It effectively provides an 'alternative pathway' to achieving Cyber Essentials Plus certification, without compromising the integrity of the scheme. Cyber Essentials works because it is clear, accessible, trusted and remains just as relevant when countering today's attacks.

Cyber Essentials Supply Chain Playbook

Attackers have demonstrated both the intent and ability to exploit weaknesses in suppliers, recognising that a vulnerability in one organisation can provide access to many others. Supply chain security is therefore an essential part of organisational resilience and the NCSC publishes a range of guidance on **managing cyber risk across complex supply chains**.

To help organisations implement Cyber Essentials throughout their supply chains, the NCSC launched the Cyber Essentials Supply Chain Playbook. The Playbook provides practical guidance on embedding cyber security requirements into procurement and supplier management processes.

Alongside this, the **Supplier Check Tool** has been created to allow organisations to check the Cyber Essentials and Cyber Essentials Plus certification of large numbers of their suppliers and contractors.

Over the past year:

- **797 large organisations** registered to use the tool
- **123 demonstrations** were delivered by mid-July 2026
- **more than 1.5 million** supplier searches were completed

Together, these tools provide practical ways for organisations to identify gaps in supplier assurance and reduce cyber risk across complex supply chains.

Defence Cyber Certification (DCC)

The launch of the DCC marked a significant step forward in strengthening the cyber resilience of the UK Defence supply chain. Developed by the Ministry of Defence, defence suppliers and IASME, DCC replaces reliance on supplier self-attestation with independent assurance, providing Defence with greater confidence that organisations handling sensitive information and supporting critical capabilities are meeting enhanced cyber security requirements for all their critical business functions. DCC uses four cyber risk profiles which incorporate Cyber Essentials within the baseline, so Defence can apply proportionate assurance while aligning more closely with recognised frameworks (such as the CAF) and NIST standards.

The NCSC played a key role in supporting the development and rollout of DCC, helping to shape the cyber resilience requirements that underpin the scheme and engaging extensively with Defence stakeholders. The introduction of DCC is transforming how cyber risk is managed across the defence industrial base by creating a consistent and measurable standard for supplier assurance. This drives greater accountability and investment in cyber resilience among suppliers, while reducing the likelihood of supply chain vulnerabilities being exploited to disrupt Defence operations. As DCC becomes embedded within Defence procurement and assurance processes, it is strengthening the security and resilience of the organisations that underpin UK Defence capabilities, helping to safeguard operational effectiveness and national security.

Helping Boards to govern cyber risks with confidence

Technology and digital systems are at the heart of modern business, driving innovation, growth, and competitiveness. As organisations adopt emerging technologies, they also introduce new risks - cyber risk being one of the most significant.

The **NCSC's Cyber Security Toolkit for Boards** remains the UK government's key resource to enable Boards to govern cyber risks with confidence. It helps members to ensure that cyber resilience and risk management are embedded throughout an organisation, including its people, systems, processes and technologies. Additionally, our **Cyber Governance Training** supports Boards and Directors in understanding the principles of the Toolkit and putting its recommended actions into practice without delving into the technical detail. These resources are supported by the government's **Cyber Governance Code of Practice** which shows boards and directors how to manage digital risks and protect their organisations from cyber attacks.

The NCSC is constantly updating its offerings to board members so that senior leaders can stay ahead of the threat. This includes:

Frontier AI: what you need to know

AI is no longer a distant or speculative issue for cyber security. The most advanced AI tools, often referred to as frontier AI, make it easier, faster and cheaper for even low-skilled hackers to carry out sophisticated cyber attacks.

The **NCSC'S Frontier AI resources** includes key messages for leaders and board members, together with resources to share with your technical experts.

Key messages for leaders and board members

AI is making it easier and faster for criminals to attack those organisations that do not have basic cyber security protections in place.

- The NCSC believes that **AI will ultimately be a 'net positive' for cyber security**, but the path to reaching this point requires urgent action now and board-level engagement.
- The rise of agentic AI tools (a new class of frontier AI) means **organisations need to understand how they are used**, and what access they have to systems and data.
- Maintaining good cyber security fundamentals remains the best way to protect your organisation from all digital threats, whether those are AI-assisted or not.

If you're new to AI, **Frontier AI: what you need to know**, provides a selection of key resources that will help you - as a leader - to keep pace with key developments.

A framework for recovery

A highly disruptive incident can feel overwhelming. The NCSC's new guidance on **Recovering from a highly disruptive cyber attack**, provides a framework for response and recovery. It's been created for organisations where the loss of critical digital systems would have significant operational consequences.

It will be particularly useful for:

- executive leaders, boards and senior decision-makers
- CISOs & cyber security teams
- CIOs, CTOs & technology leaders
- service owners
- business continuity, resilience and risk professionals

The guidance is divided into 3 sections which mirror the typical response and recovery phases:

- **Section 1** sets out the immediate activities to undertake in the first few hours to contain and assess damage, implement governance, and establish lines of communication.
- **Section 2** guides you in setting up and running your recovery programme and supporting activities during the first few days, and potentially weeks.
- **Section 3** focuses on the organisational rebuild phase which is when your organisation begins to recover its processes and is operating its business as usual.

Preparing for a vulnerability patch wave

Whether they are technology producers and vendors, or consumers and operators, all organisations have 'technical debt'; a backlog of technical issues – that is both expensive and time-consuming – as a result of prioritising short-term gains over building resilient products. Artificial Intelligence, when used by sufficiently-skilled and knowledgeable individuals, is showing the ability to exploit this technical debt at scale and at pace across the technology ecosystem.

This is why we are encouraging all organisations to **prepare now for when a 'patch wave' arrives**; a rush of software updates that will need to be applied across the technology stack to address the disclosure of new vulnerabilities. Organisations should make plans to deploy software security updates quickly, more frequently, and at scale, including across their supply chains. We are expecting an influx of updates to address vulnerabilities across all severities, and expect a number to be critical. A good place to start is by reading the NCSC's updated **Vulnerability Management guidance**.

Preparing for the quantum transition

The transition to post-quantum cryptography (PQC) will be one of the largest technology migration challenges over the coming decade. For operators of critical services, organisations holding sensitive information, and those managing complex technology environments, preparation should begin now.

Leaders should ensure that their organisation:

- understands where cryptography is used across critical systems, services and supply chains
- has ownership and governance arrangements in place for PQC migration
- incorporates PQC considerations into technology refresh and investment programmes
- develops migration plans in line with NCSC guidance and timelines
- engages suppliers and technology partners to understand their preparedness

The NCSC recommends completing discovery activities and migration planning by 2028, undertaking priority migration activities by 2031, and completing migration to PQC by 2035.



In December 2025, the NCSC and Vodafone, with the **National Cyber Advisory Board**, hosted the first UK government and industry workshop focused on PQC migration. The event brought together security leaders and those responsible for PQC in their organisations from across industry, academia and government. This energising and inspiring day reinforced a simple but critical point; **no organisation can navigate the shift to PQC alone**.



THE FUTURE OF CYBER DEFENCE

Cyber security is moving from periodic, human-led activity towards continuous, machine-assisted defence.



The changing nature of operational cyber defence

Cyber security is moving from periodic, human-led activity towards continuous, machine-assisted defence operating at national scale. This is the direction of travel that is outlined in the government's Cyber Shield concept: using data, partnerships and AI-enabled capabilities to help understand collective vulnerability and detect and disrupt threats.

For organisations, vulnerability management will no longer be limited to periodic scanning. Vulnerability discovery, prioritisation, remediation and verification will become part of an interconnected pathway. Penetration testing and assurance can also become continuous and more accessible, although they will still need direction and well-engineered safeguards to avoid unintended impact.

Security operations can move beyond presenting alerts to analysts, with agents helping to investigate activity, correlate evidence and recommend, or in some instances, take reversible action. Threat intelligence will become more contextual and timelier as models process larger and more diverse datasets, but provenance and confidence will remain essential.

Even with reimagined AI cyber defence, cyber incidents will be experienced, but response can become faster through machine-supported diagnosis and containment. But it is important to implement this alongside rehearsed playbooks, with reliable/high integrity telemetry and clear authority to act within guardrails. The future of cyber defence will depend on combining human expertise, trusted partnerships and AI-enabled capabilities.

The National Detect Strategy:

Building the future of cyber defence

The UK's critical services are frequently vulnerable to known cyber attacks. While significant progress has been made in strengthening cyber resilience, organisations across the UK continue to be exposed to common vulnerabilities and well-understood attacker techniques.

To address this challenge, the NCSC is piloting the **National Detect Strategy (NDS)**: a long-term national approach to improving the UK's ability to detect and respond to cyber threats. The strategy supports defenders in tackling known vulnerabilities and adversary tactics, techniques and procedures (TTPs) across critical systems and networks.

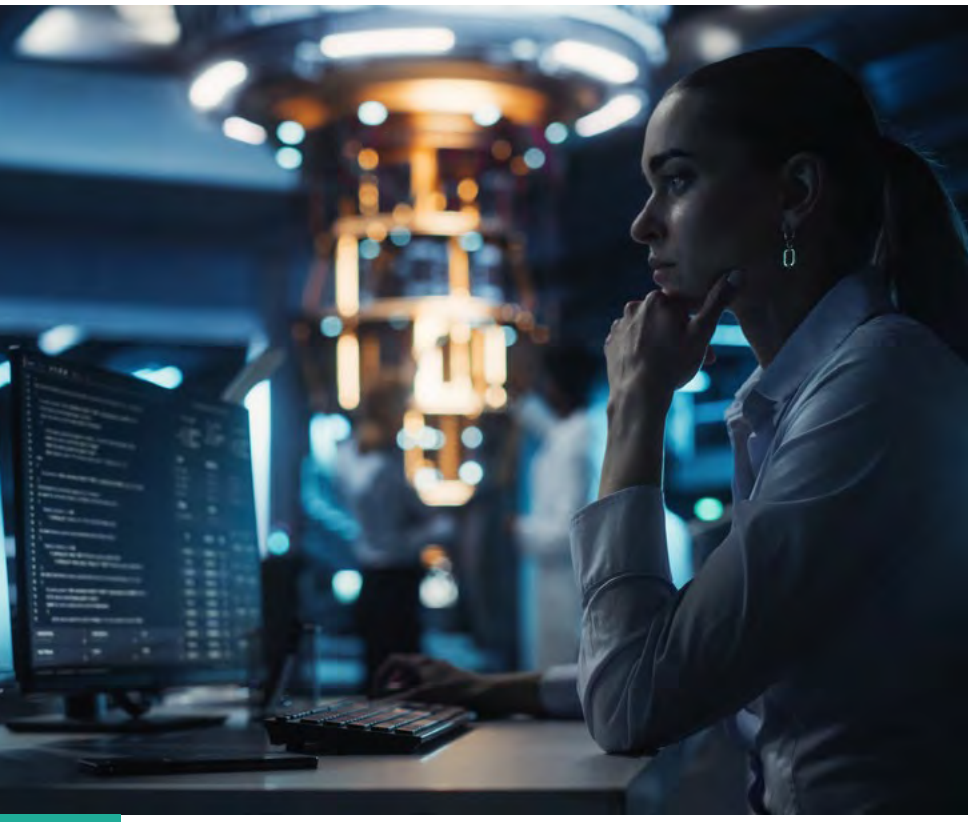
The NDS provides a joined-up approach to cyber defence, bringing together operators, oversight bodies, technology providers, government and academia to strengthen detection, share expertise and improve resilience. It focuses on challenges that are beyond the ability of a single organisation to address alone and therefore require collective action. The NDS is a key part of the Government Cyber Action Plan (GCAP) and the forthcoming National Cyber Action Plan (NCAP).

What is the NDS seeking to achieve?

By 2030, the NDS aims to deliver two national outcomes:

1. Defenders are detecting and responding effectively to known vulnerabilities and adversary tactics, techniques and procedures (TTPs) across critical systems at organisational, community and national scale.
2. Defenders have access to the capabilities, tooling and expertise required to detect and respond effectively to cyber threats.

The strategy is built around four themes that will help shape how the UK detects and responds to cyber threats in the years ahead.



1. Significantly strengthened defender communities

Defender communities help organisations combine knowledge of adversaries, vulnerabilities and technologies of common interest. The aim is to optimise scarce specialist skills through collaboration, creating a federated model that scales from individual organisations through to the national level. The NCSC is currently working closely with three key defender communities in this phase of the pilot, with plans to expand this in the future.

2 National Cyber Coordination Function (NCCF)

The strategy recognises the need for greater coordination and action at national scale. A National Cyber Coordination Function (NCCF) will help support defender communities, improve collaboration and strengthen collective responses to cyber threats. This is being explored through HUNT, which brings together the UK's national defender communities to share hypotheses and develop new tradecraft. Over 160 participants from government and industry, participated in Microsoft-led guided threat hunts. Future events will focus on

identity and TTPs associated with recent attacks.The NCSC is currently developing a wireframe of the NCCF, piloting essential functions with partners.

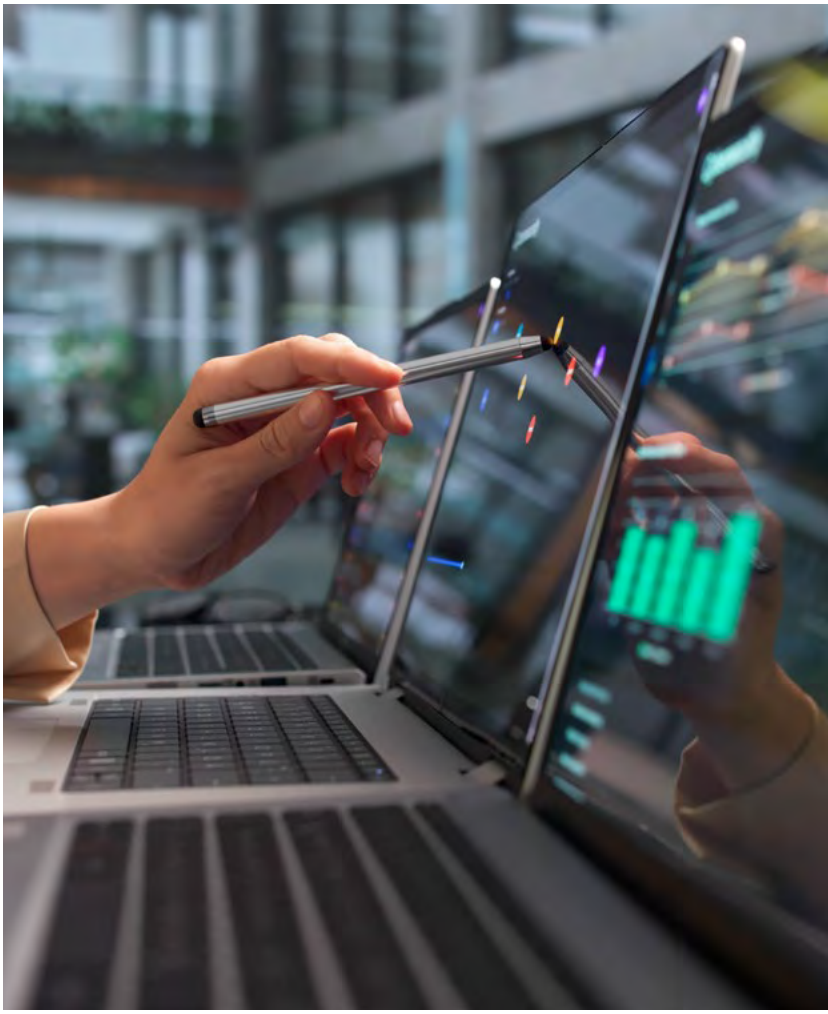
3. Improving national observability

Today, it remains difficult to establish an authoritative picture of significant cyber intrusions, exploitation and vulnerabilities affecting the UK. The strategy seeks to improve transparency and observability, enabling faster and more informed decision-making. The NCSC is currently working with major vendors and technology leaders, to establish the authorisations and frameworks needed to support greater national visibility.

4. Partnerships with industry and academia

Technology providers, researchers and academic institutions play a critical role in strengthening cyber defence. The strategy will work with partners on:

a. Application of frontier capabilities with partners, including the research and innovation needed to enable cyber defence for the AI era. The government's Cyber Shield work is exploring how agentic systems can support the near real-time detection, analysis and response to intrusions and vulnerabilities, helping to shape the next generation of cyber defence capabilities.



b. Creating the right market incentives. Well-designed technology components are typically easier to secure and defend. To help address known security challenges, the NCSC is working with vendors of edge devices, including VPN gateways, firewalls and other network appliances. This work includes initiatives such as **Making forensic observability the norm for network devices**. In the future, lessons learned from this pilot could help inform the development of a Critical Technologies Code of Practice covering a broader range of technology components.

Cyber Shield:

Building the UK's agentic cyber defence ecosystem



Cyber Shield is the UK's programme to build agentic detection, analysis and response. Jointly delivered by the NCSC and the Department for Digital, Culture, Media and Sport (DCMS), Cyber Shield aims to build a national-scale agentic cyber defence ecosystem over the next five years.

Cyber Shield will use the NCSC's unique national role to provide cyber security data to defensive agents operating within UK organisations, while consuming signals from those agents to create higher-value, enriched national insights. Organisations participating in Cyber Shield will contribute to, and benefit from, a continuously improving collective defensive capability, helping to strengthen resilience across sectors rather than only within individual networks.

Cyber Shield requires new levels of co-ordinated action:

- The NCSC will provide the core platform, intelligence, data fusion, ongoing development and the enablement of new use cases.
- The defensive agents themselves will be developed and operated by the cyber security market, the open-source community and other participants across the cyber ecosystem.
- DCMS will lead the policy work needed to unlock increasingly advanced forms of agentic cyber defence, alongside engagement with industry, academia and the wider community. This includes consultation and co-design of the protocols, standards and data models that will enable Cyber Shield to scale safely and effectively.

Technological and operational challenges

Cyber Shield will be delivered in key stages. Initial operational capability will focus on enabling detection and blocking use cases. Research conducted by the NCSC and others suggests that these defensive tasks are currently more amenable to automation than more complex activities such as autonomous remediation. Focusing first on areas where automation is already practical allows organisations to realise tangible benefits while building confidence, trust and operational experience.

However, the long-term ambition is not simply to improve reactive defence. To provide more proactive protection, the cyber security community must enable the automation of defensive actions that today remain outside many organisations' risk tolerances. The challenge is not only technological but operational. Defenders need confidence that automated actions will be safe, predictable and proportionate before they can be deployed at scale.

A capability programme and a call to action

Through a series of challenges, trialled by the recently published **AI in cyber security** problem book, the Cyber Shield initiative will lay out the key areas of innovation required to deliver on the full vision and address the challenges that currently prevent agentic cyber defence operating at national scale. Key questions remain around how organisations can gain sufficient assurance to trust increasingly autonomous defensive actions. For example, how can defenders demonstrate that an automated remedial action will not cause unintended disruption? How can systems be analysed, from source code or binaries through to configuration, to specific hardening actions that reduce attack surface while minimising impact on users and services?

Solving challenges such as these will be critical to unlocking the next generation of agentic cyber defence. The programme will create opportunities for research, experimentation and collaboration focused on these Cyber Shield challenges, bringing together government, industry and academia to address them.

Investing in the UK's sovereign cyber defence capability

As cyber security becomes increasingly shaped by AI, the UK must retain the ability to understand and coordinate national cyber risk in line with its own security priorities. While commercial products will remain an important part of cyber defence, protecting the UK's most critical



systems requires trusted mechanisms for sharing insight, coordinating defensive action and understanding risk at national scale. By creating shared infrastructure, common protocols and strong partnerships across government, industry and academia, Cyber Shield aims to strengthen both national resilience and the UK's cyber security ecosystem.

Narrowing the gap between defenders and attackers

AI offers an opportunity to narrow the gap between the defender and attacker, enabling defenders to operate with greater speed, consistency and reach than has previously been possible. A longstanding challenge in cyber security is that **defensive actions rarely scale as effectively as offensive ones**. Attackers have consistently benefited from automation and growing digital complexity, allowing them to identify and exploit weaknesses across large numbers of targets. By contrast, defenders often need to assess risks individually, coordinate changes across organisations and obtain approval before action can be taken.

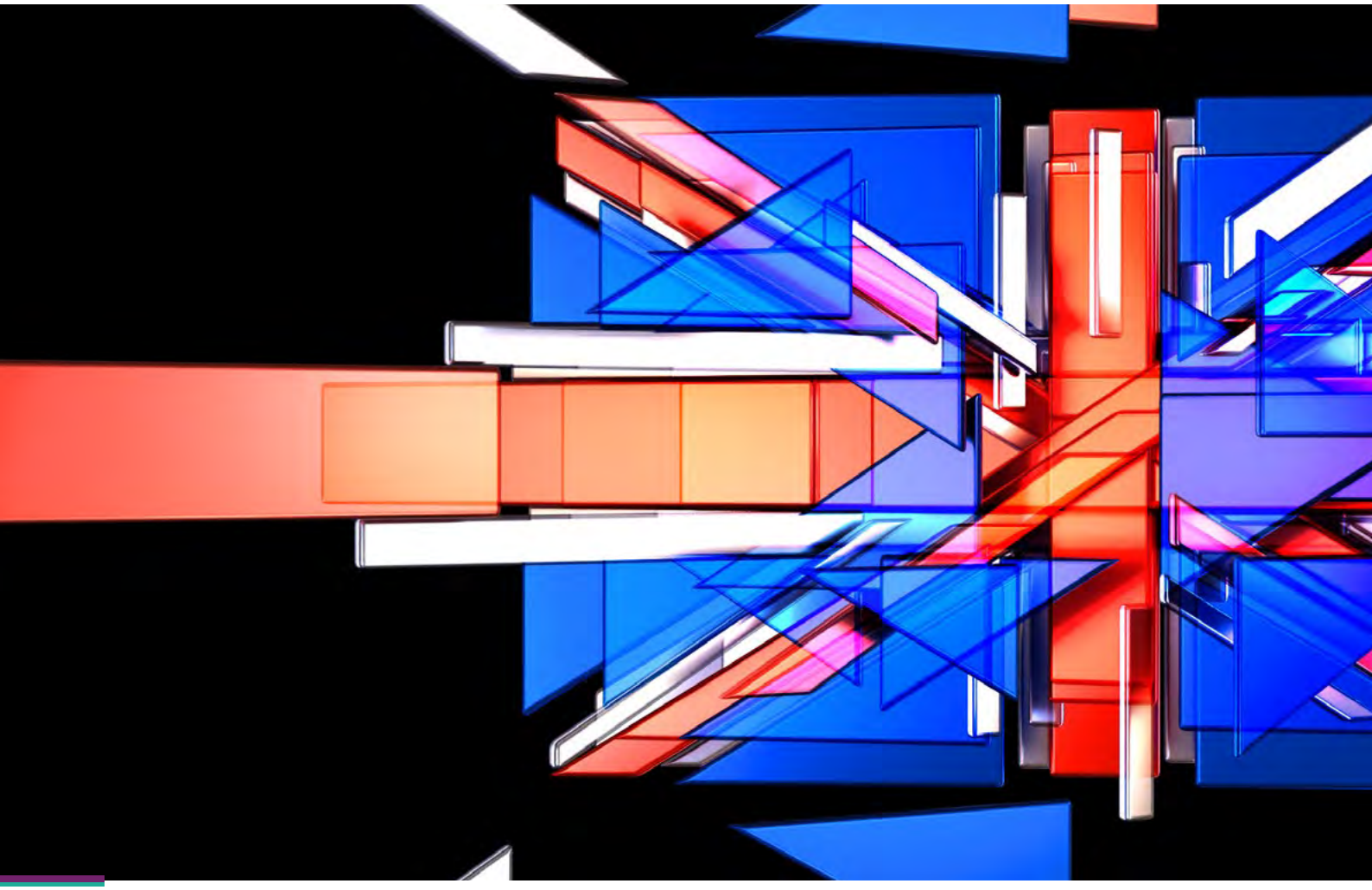
The NCSC and DCMS will lead this work, and deliver the foundational platform, but to truly narrow the gap and push the frontier of cyber defence requires anticipation, participation and a bias to action from the wider UK cyber security community. Organisations will need to integrate agents, share insights, help shape emerging standards and contribute to solving the technical and policy challenges that stand in the way of agentic cyber defence.



Project DROMOS

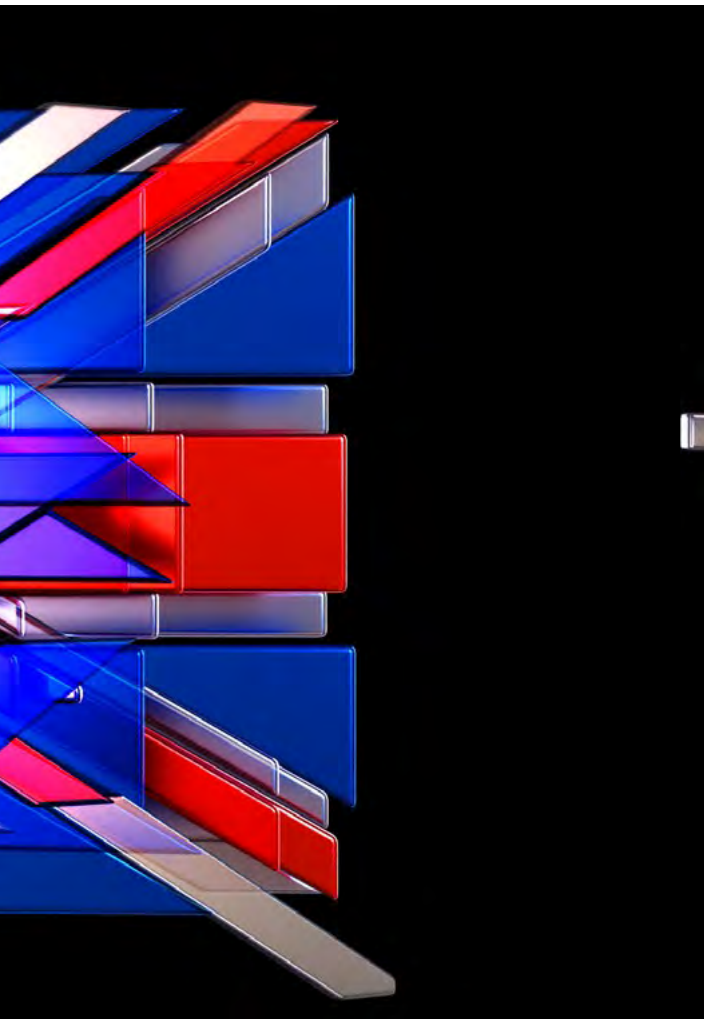
As artificial intelligence continues to transform technology, the government is exploring how this capability can also strengthen cyber defence.

In 2026, the Government Cyber Coordination Centre (GC3), a joint NCSC-DCMS enterprise, the AI Security Institute (AISI) and other government departments, launched Project DROMOS to explore how frontier AI models could help identify software vulnerabilities more quickly and effectively across government systems.



The initiative brought together cyber security specialists, software engineers and AI experts from across government to test how emerging technologies could augment existing security practices.

The programme began with a four-week pilot focused on analysing government code repositories. By using frontier AI models to review large and complex codebases, DROMOS explored how security teams could identify potential weaknesses at a speed and scale that would be difficult to achieve through manual review alone. Early results demonstrated the potential for AI-assisted vulnerability discovery, providing the confidence to expand the programme into operational environments across government.



Building on these successes, DROMOS expanded to selected government environments, where participating organisations used AI-assisted analysis to uncover hundreds of potential security issues, including critical vulnerabilities. By combining the speed of frontier AI models with expert human oversight, departments were able to assess findings, prioritise action and strengthen the security of their systems more efficiently.

Beyond vulnerability discovery, DROMOS has helped government develop a better understanding of how AI can be deployed safely and responsibly in cyber operations. The programme established governance processes, operational procedures and assurance measures to support human oversight, manage false positives and ensure AI-generated findings were handled appropriately.

The lessons learned through DROMOS are helping shape the future of cyber defence across government. As one of the first coordinated efforts to apply frontier AI models to vulnerability discovery at operational scale, the programme has demonstrated how emerging technologies can strengthen resilience, improve visibility of security risks and help protect the digital services relied upon by citizens and businesses every day.



SHAPING GLOBAL CYBER RESILIENCE

The future will be shaped by those who build the technologies the world depends on, set the standards that govern them, and bring partners together to secure them.



Shaping global cyber resilience



> ‘In an interconnected world, no nation can secure the digital future alone.’

The digital technologies that power economies, critical services and national security are global in nature, as are the threat actors that seek to exploit them. International partnerships are essential to understanding threats, building collective security and shaping the digital environment on which modern societies depend. The cyber challenge of the next decade will be shaped by both competition and cooperation. While hostile states increasingly use cyber capabilities to pursue strategic advantage, trusted international partnerships remain one of the UK’s greatest strengths.

No nation can do this alone

Over the last decade, international partnerships have become increasingly central to how the NCSC delivers its mission. What began as an important enabler to advance our objectives has evolved into a critical source of operational impact, collective influence and strategic advantage. The Five Eyes partnership remains the cornerstone of this approach, providing a uniquely trusted and operationally integrated framework for sharing insight, coordinating action and strengthening collective cyber resilience. Alongside this, our broader network



of international partners has grown in both breadth and significance, bringing together governments, international organisations and industry.

These partnerships have enabled some of the NCSC's most significant international successes. Together, we have:

- combined intelligence and expertise to provide trusted threat assessments and warnings
- exposed and attributed hostile cyber activity, raising the cost of malicious behaviour
- advanced practical approaches to cyber resilience through joint guidance and secure-by-design initiatives

More recently, our partnerships have helped set the agenda for AI security, post-quantum cryptography and the international frameworks that will shape the future of cyber security.

Partnerships as a source of strategic advantage

Defining global expectations for resilience

International partnerships make it possible to translate lessons, expertise and experience into collective action, helping to strengthen resilience across interconnected systems, services and infrastructure. In doing so, partners can achieve outcomes at scale and pace.

In practice, this means using trusted partnerships to better understand, and collectively harden, the resilience of the critical infrastructure, digital services and supply chains reducing the risk that disruption cascades across sectors or borders.

In an increasingly unstable geopolitical environment, we must recognise that we do not have the luxury of time. Any conflict we face tomorrow will be shaped by how well we prepare today. We must proactively share lessons, experiences and preparedness activities, strengthening collective readiness before periods of crisis and conflict emerge.

Beyond critical systems and infrastructure, we should align around common baseline expectations for cyber security, stimulate demand for secure products and services, and strengthen the ecosystem that delivers them. Through coordinated action against those that seek to cause harm, partners can help create a digital environment in which secure and resilient behaviours become the norm rather than the exception.

This is increasingly important because cyber resilience and economic resilience are now closely linked. Strengthening digital trust, reducing systemic vulnerability and improving resilience across global supply chains can help support growth, investment and long-term prosperity.

Making secure-by-design the norm

Together, we can ensure that security is built into the foundations of the digital ecosystem, addressing whole classes of vulnerability before they are propagated across the technologies, services and infrastructure.

In practice, this means making secure-by-design the default expectation for future technologies. We continue to manage the consequences of security not being built in from the outset, making it more important that future technologies are developed differently. By shaping the standards, frameworks and security expectations that define good security practice, and driving their adoption at scale, we can help embed security more deeply across the technology ecosystem.

It also means focusing effort on the shared technologies that underpin vast parts of the digital environment, including cloud platforms and open source ecosystems, where even small improvements can strengthen security across thousands of organisations simultaneously. Together, we can accelerate the adoption of technologies and architectures that address the source of potential vulnerabilities. We need to create the market conditions in which security becomes a defining characteristic of successful technologies, making security a source of competitive advantage and raising expectations across the wider ecosystem. Future digital foundations should be secure by design, not secured retrospectively.

Competing in the era of technological transformation

Technological transformation will sit at the heart of cyber security's evolution over the coming decade. Future advantage will increasingly depend on our ability to understand technological

change early and anticipate its implications before it becomes embedded in technology and services. Security cannot remain a response to technologies that have already been adopted at scale.

The goal is not simply to keep pace with technological change, but to shape that change to ensure each wave of innovation leaves the digital environment more secure than the one before it.

AI is the clearest example today of a technology transformation that is reshaping the digital environment on a global scale. We are already experiencing the profound impact of AI on how vulnerabilities are identified, how systems are defended and how malicious actors operate. The development of the world's first AI security standard through ETSI demonstrated how trusted partners can influence the security foundations of transformative technologies whilst they are still evolving, rather than attempting to retrofit them later.

The long-term impact of AI is still unfolding across societies, economies and national security, creating both opportunities and challenges that are not yet fully understood. The partnerships that help us respond to the realities of AI today will help determine how successfully we navigate and shape the technological transformations that follow.



Shaping the future together

Partnerships are no longer just a means of sharing information or coordinating activity. They are increasingly the mechanism through which nations shape the future digital environment itself. Maintaining and strengthening these partnerships will remain central to the NCSC's mission in the years ahead.


Ten years of making
the UK the safest place
to live and work online.
National Cyber
Security Centre
a part of GCHQ

National Cyber Security Centre
a part of GCHQ

© Crown copyright 2026.

Photographs produced with permission from third parties. NCSC information licensed for re-use under Open Government Licence www.nationalarchives.gov.uk/doc/open-governmentlicence

Designed and produced by Big+Bold

Follow us

@NCSC

@cyberhq

National Cyber Security Centre