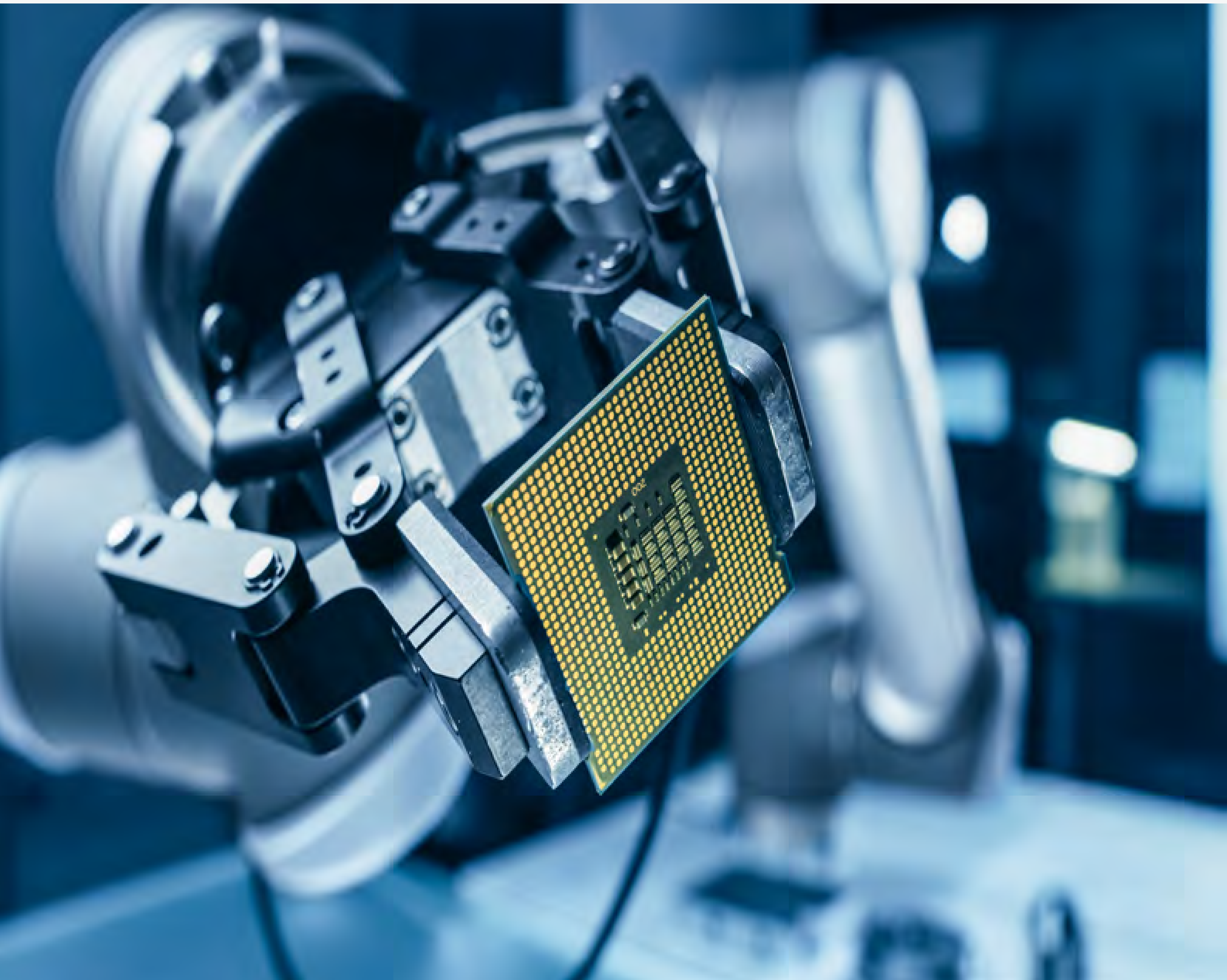
Cabinet Office

National Cyber Strategy 2022

Annual Progress Report 2022-2023



This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at ukcyberstrategy@cabinetoffice.gov.uk

Contents

National Cyber Security Centre
CYBER 2023

Ministerial foreword

It has been just 18 months since we published the National Cyber Strategy 2022 – and already, the pace of geopolitical and technological change has surpassed our already-high expectations. Russia's illegal invasion of Ukraine and rapid advancements in artificial intelligence have altered our world, with significant implications for our national security, our prosperity and our cyber power. Vital as it was in 2022, our cyber strategy is now more important than ever.

A year into its implementation, we are publishing this annual progress report to support transparency and to highlight the UK's global leadership in cyber security during this period. This report builds on the strategic priorities of the Integrated Review Refresh, demonstrating how we have adapted to the challenges of an increasingly volatile world – particularly Russia's illegal invasion of Ukraine and the rapid pace of technological change.

The UK has:

- Maintained our ongoing cyber support to the Government of Ukraine, which along with the UK is one of the most targeted nations in the world by hackers;
- Launched coordinated sanctions against cybercriminals;
- Issued an unprecedented alert to help protect our critical national infrastructure against Russian-aligned Wagner-style hacking groups;
- Set specific and ambitious cyber resilience targets for all critical national infrastructure sectors to meet by 2025;
- Set up ten formal cyber dialogues with countries across the world;
- Created a Digital and Computing Skills Education Taskforce to drive up computer science uptake in schools;
- And supported the growth of the cyber sector in a difficult economic context.

As this report shows, we are constantly having to adapt, innovate and evolve to promote the UK's cyber security, prosperity and competitiveness.

We are proud of the UK's leadership in cyber since the inception of strategy, and our core aims remain the same: to protect and promote the UK's interests in and through cyberspace, and to realise the opportunities of digital technology for our economy and our citizens. We will continue working with partners to shape a cyberspace that reflects our democratic values, and to use our world-class cyber capabilities to influence the behaviour of adversaries.

We are prioritising work across the national security community and drawing on external expertise to understand how nation states, criminals and other groups might use AI technology to conduct cyber attacks against the UK. We are also looking in parallel at the opportunities AI can offer to strengthen our cyber resilience.

To do that, we need to attract and retain the very best cyber talent in government and the wider public sector, which is why I have tasked officials to explore radical and ambitious proposals to tackle our cyber skills gap. We must deepen our already-close partnership with industry as technological change gathers pace. And we must secure our networks. As I said at the CyberUK conference in Belfast, the stronger your business, the stronger our economy, and the more prosperous we become together. In turn, we in government will continue to do as much as we can to support the cyber industry and businesses more widely. That way, we can continue to "defend as one".

Rt Hon Oliver Dowden CBE MP
Deputy Prime Minister and Chancellor of the Duchy of Lancaster

Introduction

The National Cyber Strategy 2022 set our vision for the UK to continue to be a leading responsible and democratic cyber power, able to protect and promote our interests in and through cyberspace in support of national goals.

This report reflects on key achievements and milestones since the inception of the strategy; highlighting the progress we have made alongside industry, academia and wider society, as well as looking ahead to future priorities and challenges.

It summarises our progress against the five priority actions in the National Cyber Strategy:

Pillar 1: Strengthening the UK cyber ecosystem, investing in our people and skills and deepening the partnership between government, academia and industry.

Pillar 2: Building a resilient and prosperous digital UK, reducing cyber risks so businesses can maximise the economic benefits of digital technology and citizens are more secure online and confident that their data is protected.

Pillar 3: Taking the lead in the technologies vital to cyber power, building our industrial capability and developing frameworks to secure future technologies.

Pillar 4: Advancing UK global leadership and influence for a more secure, prosperous and open international order, working with government and industry partners and sharing the expertise that underpins UK cyber power.

Pillar 5: Detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace, making more integrated, creative and routine use of the UK's full spectrum of levers.

Some of our work cannot be disclosed publicly, but the report seeks to describe our progress on implementing the strategy with insight, facts and real life case studies from colleagues across His Majesty's Government (HMG) and the Devolved Administrations.

Key achievements

since publication of the National Cyber Strategy 2022

Cyber ecosystem

Engaged over 2,000 schools, 2,500 teachers and 41,000 young people through Cyber Explorers.

Established the National Cyber Advisory Board (NCAB).

Supported over 160 companies and entrepreneurs via Cyber Runway.

3%

The cyber sector has generated 5,300 new jobs in the past year, with an increase in total annual revenue of 3%, up to £10.5 billion.[1]

Technology advantage

Published the world's first App Store Privacy and Security Code of Practice, being implemented by all 13 major app store operators.

Launched the Artificial Intelligence (AI) standards hub.

Published the Secure Connected Places Playbook in collaboration with 6 local authorities.

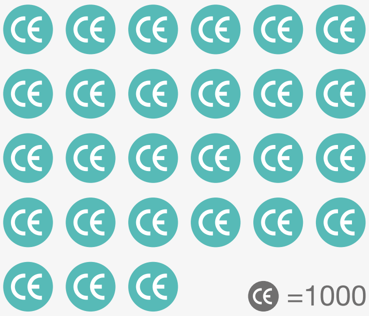
Elected to the governing Council of the International Telecommunication Union (ITU).

[1] https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2023

Resilience

Announced plans to strengthen the UK's cyber resilience legislation (the Security of Network & Information Systems Regulations).

Responded to Russia's invasion of Ukraine with support to industry and CNI operators on the heightened cyber threat.



12,000 small businesses used National Cyber Security Centre's Cyber Action Plan and over 15,000 used the new 'check your cyber security' tool.

Over 27,000 organisations certified to either Cyber Essentials or Cyber Essentials Plus.

Global leadership

Provided £7.3m in cyber support to Ukraine since the start of the invasion.

Set up formal cyber dialogues with more than 10 countries across the world as well as the EU.

Stepped up collaboration with international partners through the Counter Ransomware Initiative.

Announced a partnership with France and signed a joint statement with the US and 11 other countries on countering cyber proliferation including co-chairing the policy pillar with Singapore.

Countering threats

Took down the GENESIS marketplace, a go-to service for cyber-criminals.

Sanctioned seven Russian cyber criminals through coordinated action with the US.

Published advice and guidance, including on the threat from commercial cyber proliferation and state-aligned groups sympathetic to Russia's invasion of Ukraine.

Published 'Responsible Cyber Power in Practice', setting out how the National Cyber Force's use of its cyber capabilities aligns with our values as a responsible cyber power.

Strategic context

The period since December 2021 has seen an accelerating transition towards a world with greater geopolitical competition and multipolarity. Russia's illegal invasion of Ukraine has precipitated the largest military conflict in Europe since the end of the Second World War, with implications for the UK and NATO's approach to deterrence and defence. Russia has used offensive cyber operations to support their military campaign. This campaign has not been as effective as Russia hoped, but their activity and that of state-aligned groups has raised the risk of spillover effects in the region and beyond, including the UK. China's deepening partnership with Russia and growing cooperation with Iran are evidence of an increasingly complex international security environment. Cyber attacks by Iran on Albanian government systems in September 2022 exemplify this developing trend.

This complex international environment has continued to generate a wide range of cyber threats to the UK from our adversaries, including state and state-aligned groups. Although, we assess that the most significant threat facing citizens and small businesses, as well as the majority of critical national infrastructure providers and government service providers, continues to be cyber crime, and ransomware in particular. Last year 32% of all businesses identified at least one cyber security breach or attack.

The speed of technological development, and the size of the digital economy, increased sharply, notably for Artificial Intelligence (AI) and the Internet of Things (IoT). Meanwhile the proliferation of sophisticated commercial cyber tools and services has, as predicted, continued to drive developments in the threat, with high profile examples of their use against politicians, journalists and civil society groups.

There remains more to do to ensure that the UK economy is producing the skills that it needs to face this challenge. Approximately 700,000 businesses (51%) report a basic cyber skills gap and there is an annual shortfall in cyber security personnel of just over 14,000.[2] Our global partners share similar challenges.

But there has been progress in diversifying the cyber workforce. In 2020, it was estimated that 16% of the workforce came from ethnic minority backgrounds and 15% were female. The 2022 data shows a significant increase in these numbers to 25% and 22% respectively, with an increasing proportion in senior cyber roles (i.e. those typically requiring six or more years of experience).

[2] 'Cyber security skills in the UK labour market 2022'

The international dialogue over the rules governing cyberspace continues to evolve and is a priority for the UK. The 2022 UN General Assembly welcomed a resolution proposing a Cyber Programme of Action. This is a permanent mechanism, focused on the implementation of commitments under the UN framework for Responsible State Behaviour. Meanwhile the UK has been at the forefront of efforts to develop NATO's cyber capabilities for strengthened collective action, including enhanced civilian- military integration in cyber defence and launching a mechanism to coordinate incident response capabilities.

In response to the broader changes in the geopolitical environment, the government published the Integrated Review Refresh (IR2023). The IR2023 reaffirms the vision and strategic goals that we set out in the National Cyber Strategy. It emphasises that the UK needs to do more to build our own resilience to cyber threats and ensure we are competing at the front of the pack in the technologies that will define the next decade. IR2023 set out four ways in which the UK will protect its core national interests – shaping the international environment; deterring, defending and competing across all domains; addressing vulnerabilities through resilience, and generating strategic advantage.

The government is aligning the IR2023 with the resources and levers it needs to succeed. It is establishing a new UK Integrated Security Fund (UKISF) which will combine the existing Conflict, Stability and Security Fund (CSSF), the National Cyber Programme and a range of smaller government funds raising overall funding to £1 billion. This will integrate cross-government effort and ensure that resources are prioritised in line with IR2023 as effectively as possible.

NCS Performance Framework

The National Cyber Strategy is governed by a continuously evolving performance framework that enables a data driven approach to strategy implementation and reporting on progress.

The performance framework has several benefits:

(a) it collates data and evidence to support strategic decisions on the shape and focus of cyber programming and policy work across government;

(b) it enables the HMG cyber network to use evidence of 'what works' to adapt their cyber programmes and policies accordingly;

(c) it enables government departments and agencies to align their cyber programme delivery and policy work against the strategic objectives and outcomes of the strategy;

(d) in an evidence-based way, it enables us to measure and demonstrate the impact of the strategy to senior decision makers.

The performance framework has four key components:

1. An **outcome profile** for each strategy outcome that enables departments to clarify governance, sub outcomes, activities, policies, external factors, metrics and targets. Together, these profiles provide a framework to visualise the logic, metrics and qualitative progress markers to measure each outcome.
2. A data driven **reporting template** for pillars and outcome owners to complete every six months.
3. A **performance scorecard** that uses a mixture of objective evidence and professional judgement to determine a RAG rating status for each outcome.
4. A cross strategy **performance dashboard** to succinctly visualise evidence for senior audiences and a dashboard for each pillar to enable evidence-based decisions.

The performance framework brings together a lot of cross-government data on cyber (e.g. there are currently 120 indicators). We have moved away from a manual process to a more automated digital process to organise, manage and use the data to inform decisions at multiple levels. The performance dashboard summarises performance returns into a user friendly and succinct 10-page digital format that is more easily digestible for decision makers.

Pillar 1: Strengthening the UK cyber ecosystem

Key achievements and priorities

Since the publication of the strategy, we have established the National Cyber Advisory Board (NCAB), made new inroads into tackling the cyber skills gap, and increased the geographic reach of our support to the cyber sector.

The Prime Minister's focus on technology, the creation of the Department for Science Innovation and Technology (DSIT) and the establishment of a new taskforce for computing skills and education put the UK in a much stronger position to start closing the national cyber skills gap. Meanwhile, initiatives funded by the national cyber programme reached ever more individuals and businesses. The UK cyber security sector is now worth £10.5 billion (up 3% on last year) with nearly 2,000 businesses (up 8%).

As trailed by the Deputy Prime Minister in his speech at CYBERUK 2023,[3] we still face challenges in the short term, particularly in the public sector, and are actively looking at how to attract and retain the very best cyber experts. This work, and delivery of recommendations from the Digital and Computing Skills Education Taskforce, will be important priorities for the year ahead. We will deliver these priorities in conjunction with industry, building our sector links through collaboration with the NCAB and broader cyber ecosystem.

Progress update

The **National Cyber Advisory Board (NCAB)** was established in 2022, co-chaired by Deputy Prime Minister, Oliver Dowden, and Chief Security Officer at Lloyds Banking Group, Sharon Barber. The Board has covered topics including supply chain security, ransomware and tackling skills gaps.[4] Members provided constructive challenge to the government's approach while also mobilising their networks to help make progress on national cyber priorities.

Cyber Explorers was launched and is now reaching over 2,000 schools, 2,500 teachers and 41,000 young people across the UK.

In 2022/23, **CyberFirst** provided free cyber security courses for over 4,500 KS 3, 4 and 5 students. The 2023 Year 8 CyberFirst Girls Competition saw an increase in participants compared to 2022, with over 500 state schools taking part. We are seeing the impact of the CyberFirst programme on the nation's cyber skills pipeline with 87% of bursary graduates employed in the cyber security profession.

As part of a broader push on technology skills, a **Digital and Computing Skills Education Taskforce** was established, chaired by the Department for Education and the Department for Science, Innovation and Technology. With membership from across industry and academia, this will look to identify how industry and wider government can support computing in the education pipeline, and boost participation in, and diversity of, the subject area at GCSE, A-Level and university.

[3] https://www.gov.uk/government/speeches/cyberuk-speech

[4] https://www.gov.uk/government/news/national-cyber-advisory-board-meets-at-cyberuk-2023

From 2024, the **Digital Support Services** (Cyber Security) T-level will include an occupational specialism to provide young people with hands-on experience and help them to understand career opportunities. This T-level was developed in collaboration with cyber employers, education providers and the UK Cyber Security Council.

As announced by the Prime Minister, the College for National Security is creating a **National Security Curriculum** to be shared across the community, at multiple classifications. Cyber will be one module in that curriculum. This will help to build cyber expertise more widely and ensure that cyber experts are integrated more effectively into the broader policy community.

The Scottish Government's Strategic Framework for a **Cyber Resilient Scotland** sets out a vision of how Scotland can thrive by being digitally secure and resilient. As part of the ongoing activities, CyberScotland Week – which has grown year on year since 2018 – had 133 events across Scotland, aiming to improve cyber resilience knowledge and behaviours, and promoting skills development and careers in cyber security.

The **UK Cyber Security Council** has continued to develop and promote its work to establish nationally recognised standards for cyber security professionals. The process for awarding Chartered Status is being piloted, with the first two routes for cyber risk and architecture practitioners being delivered in partnership with information security organisations (ISC)2 and the Chartered Institute of Information Security.

Over 160 companies were supported by **Cyber Runway, a government and industry partnership that helps entrepreneurs, startups, SMEs and scaleups across the UK grow their cyber businesses,** including an £18.9 million investment in Northern Ireland's Cyber Security and AI ecosystem.

Since its launch at CyberUK in April 2023, the NCSC's **Cyber Advisor** scheme has so far onboarded 44 companies as assured service providers. These companies are located across the UK and are able to provide cost effective advice and practical support predominantly to smaller organisations wishing to implement the five Cyber Essentials technical controls but lacking the expertise to do so themselves.

In the past year, **NCSC For Startups** has been represented at conferences globally. Members of the startup community have cross-collaborated on contracts and between them, to date, the 66 companies who have gone through the programme have raised more than £468m in investment and created over 1500 jobs. NCSC's academic accelerator programme, CyberASAP, concluded its sixth cohort in February 2023, having now helped establish nearly 30 start-ups that have raised over £19 million of further investment.

In March, we delivered the first NCSC Cyber Security Education Ecosystem conference which brought together 150 representatives from academia, government and industry to explore collaboration opportunities. We have published calls for both Academic Centre of Excellence in Cyber Security Education and Research recognition in 2023. We've continued to certify high-quality cyber security degrees and now certify 54 Masters degrees, 16 Bachelors degrees and 5 Degree Apprenticeships available across the UK.

DSIT has invested in the UK Cyber Cluster Collaboration (UKC3) to help ensure all parts of the UK have a strong and vibrant cyber sector. There are now 13 UKC3-recognised "cyber clusters" across the country delivering a range of projects to boost growth, improve cyber security skills and increase innovation and collaboration. The UK cyber security sector is now worth £10.5bn (up 3% on 2022) with nearly 2,000 businesses (up 7.7%). The sector has generated an additional 5,300 jobs in the past year, with employment now at 58,000.

NCSC again hosted the UK's flagship cyber conference, **CYBERUK 2023** with the Deputy Prime Minister giving the keynote speech. The event was held in Belfast for the first time, completing a tour of each of the four nations of the United Kingdom, and helping to showcase local and UK-wide talent, skills and innovation. The conference welcomed 2,300+ cyber security professionals from 38 different countries. The event was rated as good or excellent by 93% of delegates, with 81% making three or more new connections.

We have **embedded diversity objectives across our programmes,** including:

- The NCSC has now recognised 95 CyberFirst schools and colleges across Scotland, Wales, Northern Ireland, NW, NE and SW England.
- CyberFirst North West has generated £1.57 million of social impact in less than 12 months. CyberFirst has focused on some of the most disadvantaged and deprived communities in Greater Manchester and Lancashire, with over 35% of the students supported by the pupil premium.
- The 2023 Year 8 CyberFirst bursary recruitment campaign offered 42% places to female candidates and 23% to ethnic minority candidates.
- Around half of the young people registered for our Cyber Explorers programme are female, and 32% are from ethnic minority groups.
- Half of the 160+ companies supported by our Cyber Runway programme have female co-founders and more than 40% have ethnic minority co-founders.
- The second phase of the National Centre for Computing Education is delivering a Gender Insights Programme, aimed at encouraging more girls into computing and reaching over 1,600 secondary schools.
- In Scotland, the 'Empowering Women to Lead Cyber Security' programme has provided training across the public, private and third sectors. To date, 89 women have graduated from the programme, in addition to 18 who successfully completed the iteration of the programme specifically designed for the Scottish public sector, Women in Cyber – Leading Change in Scottish Public Sector. Further cohorts will graduate later in 2023-24.

Case study
CyberFirst Schools – extending across the UK

We have started to extend the CyberFirst Schools programme across the UK. Over the last year we have reached the North East, North West and South West of England, as well as Wales and Northern Ireland. CyberFirst programmes work best when delivered locally, engaging local businesses, universities, law enforcement and others to support schools to inspire and nurture talent by supporting young people to gain the skills, experience, and exposure they need to be the future first line of defence in our CyberFirst world. Industrial partners have stepped forward, not only offering the time and energy of their staff, but also making significant financial contributions to make CyberFirst a successful government-industry partnership.

Education Scotland (Scotland’s education agency) has signed a partnership agreement with the NCSC to be the CyberFirst partner in Scotland, and are in the process of awarding the first seven schools in Scotland as CyberFirst Schools (levels of the awards to be agreed with the NCSC). The Scottish Government has worked with the digital technology trade body ‘ScotlandIS’ to provide small grants to upskill cyber professionals in all sectors. Since 2021, 335 individuals from 103 organisations have used grants to gain professional certification.

Looking ahead

We must develop interventions that are self-sustaining. To meet this challenge we will need to optimise working relationships across the cyber sector, academia, business, the Government and the Devolved Administrations.

This will include:

- Embedding the NCAB as a driving force behind the implementation of the strategy and a mechanism for helping us adapt and update our approach.
- Working with the Digital and Computing Skills Education Taskforce to develop lasting improvements to the pipeline of deep technical skills in computer science, with announcements in the next 12 months.
- Engaging with regional ecosystems across the UK to support the delivery of the government's national cyber and levelling up strategies. And exploring opportunities for further UK government funded innovation and skills initiatives, for example to support the establishment of the National Cyber Force (NCF) in the North West.
- Supporting the UK Cyber Security Council to produce professional standards to underpin the needs of the cyber workforce. This work will need to accelerate in its second year in order to achieve the strategic ambitions set out in the national strategy.
- Building on international momentum around professional standards, collaborating with European and Five Eyes partners to shape the cyber profession beyond the UK.
- Enhancing the links between the NCAB and Academic Centres of Excellence in Cyber Security Research and Education; and improving the partnership structures surrounding the Academic Centres of Excellence in Cyber Security Research.

Pillar 2: Building a resilient and prosperous digital UK

Key achievements and priorities

We set new, more specific ambitions to improve the cyber resilience of our critical national infrastructure (CNI), most recently referenced in the Deputy Prime Minister's speech at CYBERUK 2023. We launched the Government Cyber Security Strategy; the government's new cyber assurance scheme, GovAssure; and Check Your Cyber Security, a suite of free online tools enabling businesses to check if their system has any known vulnerabilities that could be exploited.

We continued to build our understanding of the way that UK businesses, organisations and citizens deal with cyber security. This includes the latest Cyber Security Breaches Survey, and the Cyber Security Longitudinal Survey, part of a 3-year study examining the cyber security behaviours of organisations and how these affect the likelihood and impact of a cyber incident.

But we have much further to go, and in the year ahead we will continue to press for progress towards higher levels of cyber resilience, particularly for government and CNI. We will take action to protect all internet users in the UK at scale, and provide greater support and incentives to the wider economy where it is needed.

Progress update

Ministers agreed to set specific and ambitious cyber resilience targets for all **Critical National Infrastructure (CNI)** sectors to be achieved by 2025 and we are examining plans to bring all private sector businesses working in CNI within the scope of cyber resilience regulations. Existing proposals to strengthen UK cyber security laws, which were the subject of a public consultation last year, will be incorporated into the Network and Information Systems (NIS) Regulation as soon as parliamentary time allows.

In addition to the consultation on NIS, we ran public consultations on new **policy to promote cyber resilience** including: unauthorised access to online accounts and personal data (Cyber Duty to Protect); software resilience and security; and improved risk management for our key data storage and processing infrastructure. We are developing a Code of Practice for software vendors which sets out a minimum set of security requirements for the development and implementation of software products.

In January 2022 we published the **Government Cyber Security Strategy**, setting out in detail for the first time how we will build a cyber resilient public sector. The government then launched GovAssure, a new cyber assurance scheme, in April 2023. This will increase cyber resilience and better protect the UK government's IT systems, which run key services for the public. All government departments and a select number of arm's length bodies, will have their cyber security reviewed annually under these new, more stringent measures. Departments will be assessed by third parties to increase standardisation and validate results.

We have seen over 27,000 organisations, the highest number ever, certified to either **Cyber Essentials** or Cyber Essentials plus in the past year. This means more organisations are embedding good cyber hygiene and can help to prevent a large number of unsophisticated cyber attacks from the internet.

We have taken steps to **reduce the burden on citizens** by building in basic protections for all and making the internet automatically safer. The NCSC now scans UK IP address ranges to help understand the vulnerability of devices and build the best possible picture of vulnerabilities that are carried by all our internet-facing devices. The NCSC's new Share and Defend capability works with Internet Service Providers to identify and block malicious websites. This capability already covers 50% of the population, and we expect to increase this figure quickly.

We have increased our **advice and guidance offering**, including a refresh of the NCSC's supply chain cyber security guidance to boards, the launch of new supply chain cyber security guidance and expanded sector-specific guidance, including for the construction sector.

We have added to our **free tools and services** with the NCSC's new Cyber Action Plan and Check Your Cyber Security tools that allow businesses to simply and quickly identify common vulnerabilities and mitigate them. We are increasingly bringing to bear our threat intelligence to protect businesses, including through the Early Warning Service, a free opt-in service that informs enrolled UK organisations of malicious activity involving their networks. This system has delivered over 34 million notifications to its 8500 and growing members to inform them of potential threats, risks, vulnerabilities or open ports in their networks.

Exercise in a Box, NCSC's free online cyber incident response exercising tool, now has 21 different exercises covering everything from Bring your own Device to supply chain ransomware. More citizen-facing 'micro-exercises' are now available without logging in. Over the last year, users signing up for the tool have increased 51% at around 20,000 users.

In May 2022, NCSC launched a new cyber incident reporting signpost service to help guide victims on where to report. We are replacing Action Fraud, the fraud and cyber reporting service, with a new service to ensure that victims can report cyber attacks and fraud to the police more easily, as well as accessing more support and information about their case.

In response to Russia's invasion of Ukraine in 2022, we took a number of steps to encourage UK organisations, CNI and the public sector to bolster their cyber resilience and preparedness. This included bespoke guidance from the NCSC on action to take when the cyber threat is heightened.

The **Devolved Governments** continue to deliver cyber resilience initiatives to drive improvements across their nations' public sectors and wider economies. The Welsh Government recently published its Cyber Action Plan which provides a consistent and coherent strategic direction for cyber in Wales.

Case study
Cyber Aware / Check Your Cyber Security

March 2023 saw the launch of Check Your Cyber Security, a suite of free online tools enabling businesses to check if their system has any known vulnerabilities that could be exploited, and detailed instructions to remedy any shortfalls. The service has already been used over 15,000 times.

Alongside this, the Cyber Aware campaign has continued to help the public and small businesses improve their cyber security. The winter campaign targeted Christmas shoppers buying goods online and helped the public understand how to avoid and report online scams. Our more recent campaign encouraged small businesses to take action to improve their cyber security, including the use of free tools offered by NCSC. There were around 100,000 visits to the Cyber Aware website during the spring campaign, with 12,000 businesses using the Cyber Action Plan.

Looking ahead

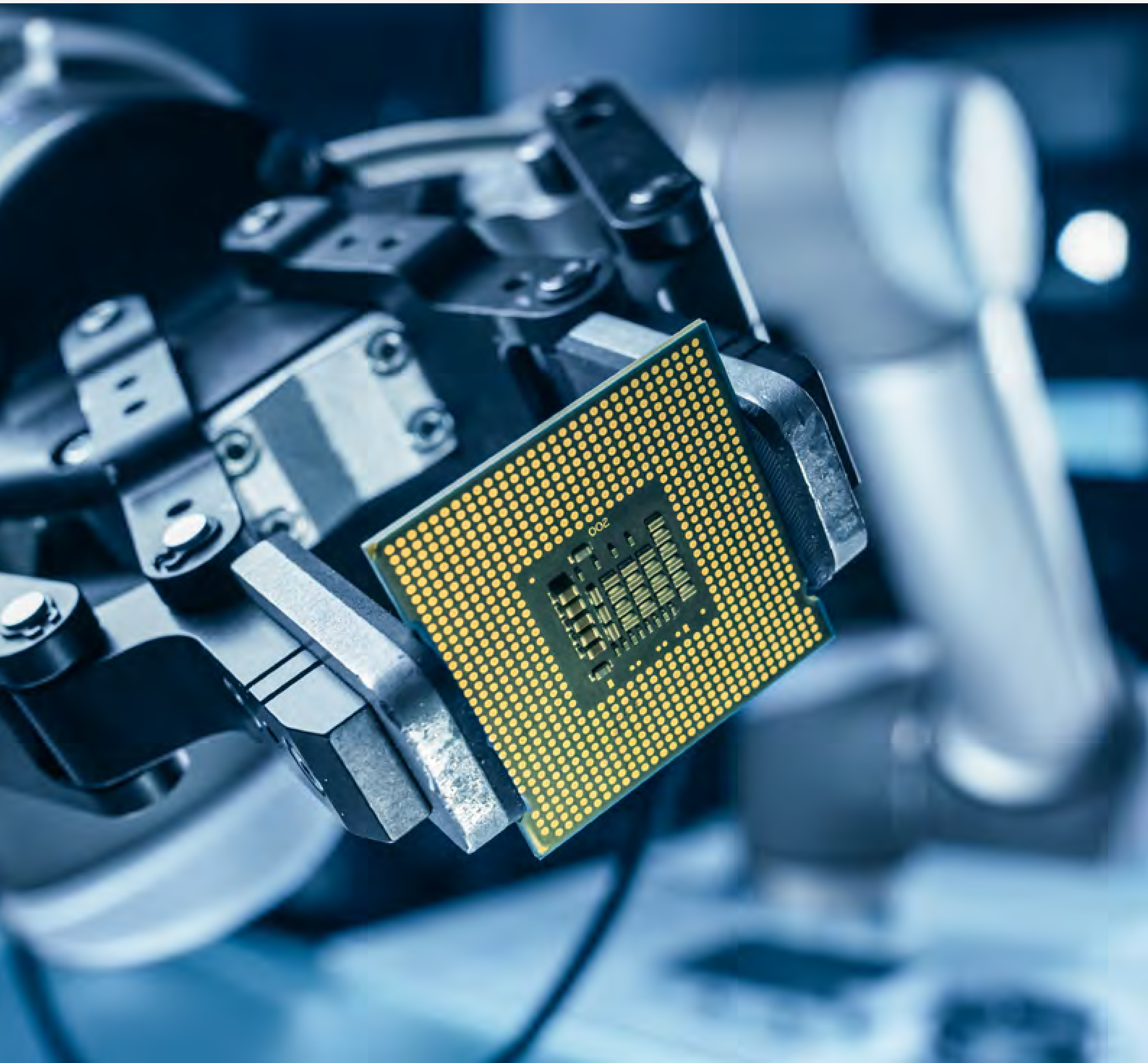
We need to shift the burden of cyber security away from the end users, and increase protections to online services that benefit us all. Close working with industry and other organisations will underpin our continued commitment to a whole of society approach to developing cyber resilience policy.

This will include:

- Increasing the reach and take up of our advice, guidance and support to businesses, organisations and individuals across the country to support them in improving their cyber defences, even in the face of increasing pressures.
- Maintaining our focus on driving up standards across the public sector and CNI, and tackling key challenges, including those posed by legacy IT.
- Further supporting and encouraging organisations to protect themselves from ransomware, the most acute cyber threat to the UK, and to report incidents when they occur to ensure they can access the support available;
- Maintaining momentum in take-up of Cyber Essentials, and continuing to take actions to promote board level engagement with cyber resilience. As announced last year,[5] we will take forward reform of audit and corporate reporting, which will introduce a new statutory "Resilience Statement" to large company annual reports including specific consideration of digital security.
- Introducing strengthened cyber security legislation through the Security of Network and Information Systems Regulations, as soon as Parliamentary times allows.

[5] https://www.gov.uk/government/news/audit-regime-overhaul-to-help-restore-trust-in-big-business

Pillar 3: Taking the lead in the technologies vital to cyber power



Key achievements and priorities

Key achievements since 2021 include gaining royal assent for the Product Security and Telecommunications Infrastructure Bill, which will place world-first obligations on manufacturers of smart devices to make them more secure, and launching the world's first Government-backed Code of Practice for App Store Operators and App Developers, which sets out minimum security and privacy requirements to protect users from malicious and poorly developed apps. In May 2023, we launched the alpha version of the Secure Connected Places Playbook. Aimed at local authorities, the playbook is a new resource offering practical and accessible support to improve the cyber security of their connected places, or 'smart cities', across the UK.

We are fostering closer collaboration with industry and international partners to champion effective and informed policies and strategies and working closely with academia in order to convert their research into technologies, products and services which benefit the cyber security sector. The creation of DSIT will position the UK at the forefront of global scientific and technological advancement and drive innovations that change lives and sustain economic growth. This new way of working has helped to ensure our work is technically backed up, validated and aligned with wider HMG priorities.

Progress update

To enable a coherent and united cyber perspective across Government on **critical and emerging technology** we have undertaken a programme of 'horizon scanning' to understand what technologies are being developed or discussed by international partners, industry, and academia; if existing technology is being used in a different way that introduces new risks; and if a technology has cyber opportunities and risks that Government needs to address. This has led to cyber considerations being included in several NetZero Government strategies and making security one of the principles in the recently published AI White Paper.

In December 2022, the **Product Security and Telecommunications Infrastructure Act** received royal assent, requiring manufacturers, importers and distributors to ensure that minimum security requirements are met in relation to consumer connectable products such as smart TVs. The Act provides a robust regulatory framework that can adapt and remain effective in the face of rapid technological advancement, the evolving techniques employed by malicious actors, and the broader international regulatory landscape. The Office for Product Safety and Standards (OPSS) has been confirmed as the intended regulator for the product security regime. They are now building up resource, capacity and market understanding ahead of enforcement regime commencement (confirmed for 29 April 2024).

The new **National Crypt Key (CK) Strategy,** agreed by Ministers in 2022, is driving activity across government to support the sovereign CK industrial base in delivering high quality products for UK use and export. A Crypt Key Company Standard will set out both the security and sovereignty standards suppliers must meet and allow HMG to track the skills and capabilities across the industry. This has now been released to industry and responses are now being assessed. We expect a significant increase in the number of recognised sovereign CK suppliers, giving HMG the building blocks for a more resilient and manageable sovereign supply base.

Since publishing the world's first voluntary **Code of Practice for App Store Operators and App Developers,** we have been working closely with app store operators to understand their adherence to the Code during the nine month implementation period. All 13 major operators have started to implement the Code of Practice, and we have requested feedback on implementation.

We have published the **National Semiconductor Strategy,** which sets out how an initial £1 billion of government investment will boost the UK's strengths in design, research and advanced chip leadership. This includes continuing to support the world-leading Digital Security by Design programme, which is making semiconductors more resilient and secure in the face of growing cyber threats.

We continued to show leadership internationally by demonstrating and sharing cyber policy work with other countries and supporting capacity development through key **multilateral institutions**, such as the G7, the Organisation for Economic Co-operation and Development (OECD) and International Telecommunication Union (ITU). In 2022, we secured a seat on the ITU Council, the governing body of the UN specialised agency for Information and Communication Technologies, with the second highest number of votes in the Western European region. This enables the UK to drive forward ITU reforms and support the ITU's core mission to bridge digital divides, enhancing our ability to shape a collaborative, effective and respected organisation which delivers for all.

We have also contributed to the development of **OECD Recommendations on Digital Security,** to support stakeholders in developing digital security policies for economic and social prosperity – including in securing digital products and services and managing digital security vulnerabilities. We are working to secure commitments through the G7 to continue close cooperation and alignment in securing critical and emerging tech, including IoT, apps and software. Through G20, we are shaping a positive role for G20 members around digital security to unlock growth and innovation in the economy.

In October 2022, we launched the **AI Standards Hub**, led by The Alan Turing Institute, the British Standards Institution and the National Physical Laboratory. The Hub is the first of its kind initiative to increase the voice of the UK in global AI standards by supporting stakeholders to learn about and engage in AI standards development processes. We have also made significant progress in making global standards development organisations, such as the Internet Engineering Task Force, more accessible to a wider range of stakeholders.

The NCSC launched **Principles Based Assurance (PBA),** which supports manufacturers to demonstrate competence, and buyers to gain confidence, in the cyber security of technology. In addition to developing a route for self-assertion, we have begun a programme of work to stand up Cyber Resilience Test Facilities (CRTFs) which will allow independent assessment of vendors and products using the PBA framework. We are exploring international recognition for this process.

Case study
Enterprise connected devices

We have undertaken work to understand the cyber security of enterprise connected devices including the ‘smart’ products increasingly used in office environments. If compromised, these devices could offer an attacker access into a business and its sensitive data. In October 2022 we launched a research project with NCC Group into potential vulnerabilities in popular devices used by UK businesses to better understand their cyber security risks. These devices were tested against existing security principles and guidance to understand how robust these are for facing evolving threats. Emerging findings from the draft report include:

- Outdated software was prevalent across devices, with one example being over 15 years old.
- Identification of 1 critical and 9 high risk vulnerabilities identified across 8 tested devices.
- Some identified vulnerabilities would have enabled the use of features such as full access to a camera, being able to monitor/record VoiP calls.
- Higher price is not an indication of better security, and long-term consideration should be given to further legislation.

This report will sit alongside existing pieces of research that we have commissioned to help us better understand relevant dynamics. We will continue to work with subject matter experts and NCSC to better understand the risks of enterprise connected devices, and what can be done to improve their level of cyber security. As part of this, we are planning a public consultation to seek feedback on our work to date, and to understand stakeholder sentiment towards different possible interventions that could help improve the cyber security of these devices.

Looking ahead

We recognise the wide-ranging impact that technologies continue to have on our lives and are embedding cyber security into technologies of today, and of tomorrow, such as artificial intelligence and quantum. One essential feature of our work is to acknowledge that these technologies can both enhance cyber security and amplify cyber risks. For example, adversarial cyber attacks can manipulate artificial intelligence algorithms, leading to false positives or evading detection.

We will be taking further actions in the following areas:

- Building on the UK's leadership in AI, the new expert taskforce backed by £100 million and hosting of the first major global summit on AI safety in the autumn, we will work to secure AI and machine learning technologies while encouraging innovation to thrive in the UK.
- Communicating a clear strategy on setting up a national laboratory for operational technology (OT); and aligning policy work and next steps on OT against the backdrop of wider initiatives.
- Promoting the rapid and widest possible uptake of new memory secure microprocessor technology that has been realised through the Digital Security by Design programme for the benefit of cyber security.
- Gathering further evidence to understand the impact of the Product Security and Telecommunications Infrastructure (PSTI) Bill.

Pillar 4: Advancing UK global leadership and influence

Key achievements and priorities

Key achievements since 2021 include: working with our international partners to call out and tackle malicious cyber activity and further build consensus around the application of rules, norms and principles in cyberspace, including hosting an international conference on Responsible Cyber Power in Wilton Park; working closely with international partners to tackle the threat from ransomware, for example, through participation in the International Counter Ransomware Initiative (CRI) led by the US; collaboration with eleven other countries in signing the US joint statement on countering the proliferation and misuse of commercial spyware; and continued partnerships with the governments of Australia, Canada, the Netherlands, New Zealand and the United States to deliver the UN Women in Cyber fellowship.

In the next period, we will work with France and the US to spearhead a broader effort to **counter the malicious use of cyber tools** to undermine our security and human rights; and continue to support Ukraine's cyber resilience, protecting them against cyber-attacks.

Progress update

The UK continues to demonstrate unwavering **support for Ukraine** against Russia, as we work with our allies to ensure that Ukraine's cyberspace is protected. With our support, critical Government of Ukraine networks remained online and operational during the Russian invasion, even as they dealt with hundreds of cyber incidents. In 2022/23, the UK bolstered Ukraine's cyber defences, providing £7.3m in cyber support since the start of the invasion. Alongside this, we continued our cyber deterrence efforts against malicious state and non-state actors.

We have prioritised UK action to address the threat from commercial **cyber proliferation,** sharing UK assessments about the threat with international partners, as well as initial plans for further action where the UK can play a leading role. At the UK-France Summit on 10 March we announced a UK-France partnership on this issue. Further at the Summit for Democracy we publicly signed a declaration on coordinating efforts with 11 other countries.

We have updated and republished the **UK Deterrence Toolkit,** to set out our approach and serve as a tool in discussions with international partners. We firmly believe that hostile states engaged in malicious cyber activity need to be aware that there are costs associated with this activity.

The UK has continued to deliver **cyber capacity building** support internationally, through programmes in Ukraine, Georgia, the Indo-Pacific, India and Africa. These programmes have supported our international partners to have stronger capabilities, stronger cyber hygiene, political resolve, governance and systems for investigating and disrupting cyber threats as well as building resilience, in turn resulting in a reduced threat from abroad to UK citizens. We have delivered this in collaboration with partner countries, including through the EU's Cyber for Development project and the Global Forum on Cyber Expertise. Commonwealth countries have also benefited from UK cyber security capacity building activity during the UK's term as Chair-in-Office (2018-22), **delivering over 140 events in 32 countries, training over 6,000 people.**

At the Commonwealth Heads of Government Meeting in 2022 in Rwanda we continued to promote the UK as a leading cyber power and secured a further £15m commitment of support until 2025. Funded by the Global Cyber Programme, the Digital Skills Community project helped build Oman's cyber resilience, develop technical skills, and raise awareness of cyber security issues and the opportunities offered through cyber security jobs by: running and publicising a national competition to test Omani student and job-seekers' cyber security skills.

As part of broader work to **counter cybercrime,** the UK, with Singapore, is leading the policy pillar of the international Counter Ransomware Initiative (CRI). We are developing four projects to address key ransomware policy challenges, around victim behaviour, virtual asset legislation, cyber insurance and incident reporting. We continue to shape discussions in the Ad-hoc Committee developing a new cybercrime treaty.

A multi-year project with the **Commonwealth Secretariat** conducted legislative reviews with countries to raise standards of cybercrime legislation, identifying gaps in legislation and providing support drafting new laws. Training was also provided on how to enforce legislation and promote cross-border co-operation on the handling of digital evidence in transnational investigations. The Africa Joint Operations Against Cybercrime project enabled the successful implementation of an operation against romance fraud in the West Africa region, resulting in arrests of threat actors who were involved in scams worth thousands of dollars, as well as the seizure of digital and mobile devices.

We have continued to expand and deepen our bilateral **cyber dialogues** and partnerships with countries across the world, as well as with the EU and the Five Eyes. In April 2022, India and the United Kingdom outlined our commitment to a joint programme of cooperation to deliver our Enhanced Cyber Partnership, focused on cyber governance, deterrence, resilience and capacity building. In May 2023, we established a UK-Japan Cyber Partnership under the Hiroshima Accord that will strengthen our public-private partnerships, advance shared international interests and enhance our cyber capabilities. In June 2023, the UK Deputy Prime Minister, Oliver Dowden, and the head of Indonesia's State Cyber and Cryptography Agency, Hinsa Siburian, also signed a Memorandum of Understanding (MoUs) to bolster cyber cooperation between the UK and Indonesia. He also signed MoUs on emerging technology and data with Singaporean Minister for Communications and Information, Josephine Teo.

We have engaged at the **United Nations (UN)** to further UK priorities and promote responsibility and inclusivity. The 2022 UN General Assembly welcomed a resolution proposing a Cyber Programme of Action. The UK remains committed to maintaining international peace and security through the development and implementation of the UN Framework for responsible state behaviour in cyberspace. In the Open Ended Working Group on information and communication technologies, the number of middle ground States actively participating has increased and UK sponsored initiatives such as the Women in Cyber fellowship have helped to improve the diversity of perspectives. To address the challenges faced by developing countries, the UK led the promotion of the Oxford Cyber Capacity-Building Model. The first UK-UN Strategic Dialogue in January 2023 saw high-level engagement on the UN Secretary General's digital and technology agenda, in particular the proposed Global Digital Compact.

The UK has been **leading efforts in NATO** to improve civilian-military integration in cyber defence. This has resulted in allies agreeing to launch a new mechanism to better coordinate cyber defence in NATO, as well as to facilitate improved engagement with the private sector. We have formally launched NATO's new Virtual Cyber Incident Support Capability (VCISC) at the Vilnius Summit to support national mitigation efforts in response to significant malicious cyber activities and increase all forms of assistance from Allies. We have also driven enhancements to NATO's Cyber Defence Pledge, which provides for a more targeted annual reporting mechanism to help allies to address vulnerabilities and be more resilient to malicious activity.

The UK hosted Defence Cyber Marvel 2 exercise, Western Europe's Largest Military Cyberspace Competition. Over 30 international teams with government, military, and industry representation came together to defend an unfamiliar network against adversaries in a real-world context, testing critical skills in a dynamic, escalating scenario.

Case study
Ukraine Programme

The UK’s Ukraine Cyber Programme has supported Ukraine’s cyber defenders to detect, limit, remediate and prevent Russian-linked cyber-attacks. The programme has worked with leading cyber security companies and government to strengthen and support Ukrainian cyber resilience against this assault, and specifically to provide incident response support to Government of Ukraine entities, protecting them against cyber-attacks, including malware such as Industroyer2. The programme is preventing malicious actors from accessing vital information relevant to the war effort. It has also limited attacker access to vital networks and supported Ukraine to harden their critical infrastructure against future attacks and delivered frontline cyber security hardware and software including firewalls, Distributed Denial of Service (DDoS) protection and forensic capabilities to enable Ukrainian analysts to fully understand system compromises.

Looking ahead

In 2022 the UK announced four new cyber programmes to complement the wider cyber portfolio. We will be focussing on these throughout the next phase of the strategy:

- **Ukraine** – to help Ukrainian cyber defenders respond to materialising cyber-attacks, limited attacker access to vital networks and harden critical infrastructure to future assault.
- **India** – to deliver the UK's and India's commitments to a programme of co-operation focused on cyber governance deterrence, resilience and capacity building.
- **Indo-Pacific** – to provide deeper capacity building of a limited number of priority countries with emerging capabilities. And supporting partnerships with cyber mature countries and regional organisations.
- **Africa** – to help deliver the objective of deepening and developing a mutual partnership with African countries, working together to build more resilient and productive economies and open societies. The Africa Cyber Programme will support partner country development with Kenya, Nigeria and South Africa by helping to strengthen their cyber resilience and security and demonstrate the benefits of a free, open, peaceful, and secure cyberspace. The programme will also fund projects delivered by INTERPOL on cybercrime and the African Union, to support the development of cyber governance processes in Africa.

Pillar 5: Detecting, disrupting and deterring our adversaries

CHECK POINT
THREATCLOUD
RECENT DAILY ATTACKS
LIVE CYBER THREAT MAP
25,527,923 ATTACKS ON THIS DAY
ATTACKS
DNS Enforcement Violation
Infecting URL.RS.TC.71a2JaTm
NTP Enforcement Violation
DNS Enforcement Violation
Barys.TC.1720xHLR
DNS Enforcement Violation
DNS Enforcement Violation
United States
United Kingdom
Portugal
South Africa
Malware
Phishing

Key achievements and priorities

Key achievements since 2021 include calling out irresponsible behaviour in cyberspace by a number of state actors; announcing sanctions for the first time against ransomware groups; the takedown of the GENESIS cybercrime market; and substantiating our commitment to transparency around the UK's National Cyber Force (NCF), with the publication of 'Responsible Cyber Power in Practice'.

We continued to grow and develop the role of the NCF and moved forward with the National Crime Agency (NCA)'s capability investments announced in the strategy. This has taken place alongside ongoing efforts to regularly share advisories with industry and operational campaigns against our adversaries which cannot be discussed in this public report.

In the year ahead, our key priorities will be continuing to learn lessons from events in Ukraine; announcing further steps on our policy response to ransomware; and further building on our success at conducting coordinated cyber campaigns against key threat actors.

Summary of progress

In line with our commitments in the National Cyber Strategy, we have continued to work with our closest diplomatic partners to **deter and disrupt malicious cyber actors.** We have strengthened our outreach to an increasing number of countries, continued to raise awareness of the threat posed by malicious actors and worked with our partners to impose costs on those who conduct malign cyber activity against us and our allies.

In September 2022 the UK, along with the US, Albania and Israel, **attributed to Iran the cyber-attack that impacted Albania** in July.[6] This was the first UK attribution of malign cyber activity to the Iranian State. We have also **called out Russia's malicious use of cyber-attacks** against Ukraine, joining 12 other countries plus the EU, to attribute Russian responsibility for an operation targeting commercial communications company Viasat.[7]

Using our autonomous Cyber Sanctions regime, the UK recently **launched groundbreaking coordinated UK-US sanctions against seven individuals involved in cybercrime,** in line with our aim to deter and disrupt state, criminal and other malicious cyber actors.[8] This started a concerted initiative to jointly impose sanctions, undertake law enforcement operations, and engage in disruptive activities against ransomware actors with the United States. It demonstrates the effective join up and deployment of law enforcement,

[6] https://www.gov.uk/government/news/uk-condemns-iran-for-reckless-cyber-attack-against-albania

[7] https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion

[8] https://www.gov.uk/government/news/uk-cracks-down-on-ransomware-actors

diplomatic, intelligence and policy expertise to deliver such coordinated action against cybercriminals, to hold individuals to account for their criminal behaviour in cyberspace.

We have also made important progress building capacity to act in cyberspace in support of UK national interests. The **National Cyber Force (NCF)** has increased its operational output, delivering operations supporting the Armed Forces and wider UK foreign and domestic security objectives, while Defence continues to mature the integration of cyber capabilities into military operations. Work continues to prepare facilities at Samlesbury, the NCF's new HQ, to accommodate its growth and meet the ambition set out in the National Cyber Strategy. In April 2023, **we published *National Cyber Force: Responsible Cyber Power in Practice,***[9] delivering on the government's commitment in the Integrated Review Refresh 2023 (IRR23) to demonstrate an open and transparent approach to our use of offensive cyber capabilities. For the first time, this provides detail on how the NCF conducts its operations daily to protect the UK, in a way that is accountable, precise and calibrated and in line with domestic and international law.

[9] https://www.gov.uk/government/publications/responsible-cyber-power-in-practice

Case study
GENESIS Market

In April 2023 the NCA supported an international operation with law enforcement partners from the United States, Europe, Australia and Canada to take down GENESIS – one of the biggest online marketplaces selling stolen credentials to criminals worldwide. The GENESIS Market hosted approximately 80 million credentials and digital fingerprints stolen from over two million people. The operation resulted in 120 arrests, over 200 searches and almost 100 pieces of preventative activity carried out across the globe.

Following the rollout of Cyber Crime capability in all UK police forces, we have undertaken an **in depth review of the cyber crime policing network.** This review included governance, operations and tasking, technology and people. A nationally led, regionally managed and locally delivered operating model has been implemented across the four Ps of Pursue, Prevent, Protect and Prepare. This will enable the cyber crime policing network to respond in a more cohesive and effective way to tackle this borderless threat.

We have continued to improve **understanding and raise awareness of the cyber threat** facing the UK and our allies. The NCSC has shared regular technical advisories,[10] drafted in close partnership with our international partners, to identify and provide the technical insight to detect and remediate specific threats posed by malicious cyber actors.

As part of CYBERUK23, the NCSC publicly released a threat assessment on **commercial cyber proliferation.** This shared government's understanding of how commercial tools are lowering the barrier to entry for state and non-state actors looking to obtain cost-effective cyber capabilities and intelligence.[11]

NCSC's recent **CNI alert** has also provided guidance to help CNI organisations understand emerging cyber threats.[12] This highlighted the risk posed by state-aligned adversaries following the Russian invasion of Ukraine and provided organisations with tools, advice and capabilities to protect themselves against cyber attacks as part of our broader resilience pillar work. In May 2023, the UK and allies issued a **joint advisory** revealing technical details about a sophisticated espionage tool, named Snake, used by Russia's Federal Security Service (FSB) against their targets for nearly two decades.[13] The advisory is designed to help organisations understand how Snake operates and provides suggested mitigations to help defend against the threat.

[10] https://www.ncsc.gov.uk/section/keep-up-to-date/reports-advisories

[11] https://www.ncsc.gov.uk/report/commercial-cyber-proliferation-assessment#:~:text=type%20of%20victims.-,What%20is%20the%20commercial%20cyber%20proliferation%20threat%3F,able%20to%20develop%20or%20acquire

[12] https://www.ncsc.gov.uk/news/ncsc-warns-of-emerging-threat-to-critical-national-infrastructure

[13] https://www.ncsc.gov.uk/news/uk-and-allies-expose-snake-malware-threat-from-russian-cyber-actors

Looking ahead

Russia's war in Ukraine will continue to complicate our threat picture. The Russian State is one of the world's most prolific cyber actors. It dedicates significant resources towards conducting cyber operations around the globe. It has undertaken a range of attacks in support of their illegal invasion of Ukraine in February 2022, and the NCSC has confirmed that Russian cyber activity has included attempted cyber attacks against the UK media, telecommunications and energy infrastructure.

We continue to face consistent threats from other adversaries in cyberspace and recognise the particular challenges we face from China and the threats posed by state and non-state actors operating from Iran and DPRK. These all pose challenges to our efforts to both detect and understand the threat; and ensure we are taking actions to reduce harm to the UK.

The UK will work with the US and likeminded partners on further sanctions delivery with the long term goal of pursuing coordinated, collective action. Progress on this is dependent on the maturity of partner countries' cyber sanctions regimes, their associated policy and our ability to secure close coordination.

The National Security Bill became law after securing Royal Assent on 11 July. This legislation includes a variety of new offences which can be applied to hostile state cyber activity, and which may open up new avenues for the prosecution of cyber actors. The NCA and NCSC will continue to work closely with international partners to break the international cybercrime ecosystem. This includes tackling the complex and evolving threat from ransomware and the ransomware-as-a-service (RaaS) model.

Understanding the threat landscape and driving further reporting of cyber crime will remain a priority and a challenge, requiring better engagement under the National Cyber Strategy's 'whole of society' push. The evidence base on cyber crime and understanding about its true cost remains limited, both in the UK and globally. The NCA currently estimates that only about 2-10% of cyber crime is reported, making it one of the most underreported crime types in the UK. Low rates of awareness, monitoring and understanding of the costs associated with cyber breaches are a contributing factor.

Cabinet Office