National Cyber Security Centre
a part of GCHQ

Annual Review 2022

Making the UK the safest place to live and work online

ABOUT THE NCSC

The National Cyber Security Centre (NCSC), a part of GCHQ, is the UK's technical authority for cyber security. Since 2016 it has worked to make the UK the safest place to live and work online and bring clarity and insight to an increasingly complex online world.

This review of its sixth year reflects highlights and milestones between 1 September 2021 and 31 August 2022, and it looks ahead to future challenges.

As part of a national security agency, not all its work can be disclosed publicly but the review seeks to describe the year with insights and facts from colleagues inside and out of the organisation.

This is an executive summary, with the full version available at **ncsc.gov.uk/annual-review-2022**

TABLE OF CONTENTS

TIMELINE

10 September
Top UK and US cyber security officials affirm commitment to tackling ransomware

6 October
Three more universities recognised as Academic Centres of Excellence in Cyber Security Education

18 November
UK, US and Australia issue joint advisory after Iranian actors found to be exploiting known vulnerabilities to attack multiple sectors

23 November
NCSC and KPMG publish second Decrypting Diversity report on progress and challenges in the cyber security industry's diversity ambitions

29 November
NCSC for Startups welcomes four more innovators

10 December
Patching and monitoring advice issued to mitigate Apache Log4j vulnerabilities

15 December
National Cyber Strategy published, calling on the whole of society to play their part preserving a free, democratic and resilient cyberspace

17 January
Guidance issued for organisations on the heightened cyber threat, in light of Russia's invasion of Ukraine

24 January
Cyber Essentials scheme refreshed and updated

28 January
NCSC reiterates need for UK organisations to prepare for 'heightened cyber alert' in response to the situation in Ukraine

2 February
NCSC joins the seL4 Foundation

7 February
A new-look CyberFirst Girls Competition crowns 13 competition winners across the UK nations and regions

9 February
NCSC, US and Australia urge businesses to take protective action against increasingly professional criminal attacks

18-24 February
UK Government assesses Russia to have been involved in DDoS attacks on Ukraine. Lindy Cameron urges organisations to strengthen their cyber defences

18 March
Latest Cyber Aware campaign launched as Suspicious Email Reporting Service (SERS) reaches 10m milestone, resulting in takedown of 76,000 online scams

18 March
NCSC urges organisations in the UK to bolster online defences in light of Russian invasion of Ukraine

10 May
UK and US attribute a series of cyber attacks to Russia against Ukraine in the hours before the invasion. NCSC's Active Cyber Defence programme publishes its "Fifth Year" paper

10-11 May
CYBERUK22 in Newport, Wales. New service launched to help organisations identify vulnerabilities that could lead to email spoofing or email privacy being breached

28 June
Lindy Cameron's speech at Tel Aviv Cyber Week on partnerships and international regulation of sophisticated cyber capabilities

8 July
NCSC and Information Commissioner's Office ask the Law Society to help tackle a rise in payments being made to ransomware criminals

25 July
A new Cyber Advisor Pilot scheme announced

MINISTERIAL FOREWORD

This year, we have seen all parts of UK society come together in support of Ukraine to resist Putin's barbaric and illegal war. That war extends to all fronts, including cyberspace. The NCSC has provided vital support to Ukraine based on its unique understanding of the heightened cyber threat. The UK is not immune. Sophisticated state actors continue to pose a significant cyber threat.

New data shows the UK is the third most targeted country for cyber attacks, behind only the USA and Ukraine. The NCSC plays an essential role in meeting this threat and making the UK the safest place to live and work online. It has also worked with government, industry and the public to bolster the UK's cyber resilience. It continues to take down online scams, as well as to advise the public on how to stay safe online, and consolidate our world-leading position in research and education.

This whole of society approach forms the core of the new National Cyber Strategy 2022. The Strategy brings together government, industry and academia in partnership, drawing on expertise from all parts of the UK, and engaging citizens in our collective effort.

As more people live and work online, we must continue to realise the opportunities of digital technology for our economy and our citizens. The National Cyber Strategy plays a critical role in driving growth and innovation, setting out our plan to cement the UK's position as a responsible and democratic cyber power. It is ambitious in pursuing a competitive advantage in the underpinning technologies that are critical to cyberspace.

As we look to the future and learn from the invaluable work of the NCSC over the past year, it is clear that we must continue to engage the whole of society to shape a cyberspace that reflects our values and realise the opportunities of a thriving digital economy

The Rt Hon Oliver Dowden CBE MP,
Chancellor of the Duchy of Lancaster

DIRECTOR GCHQ FOREWORD

We must be able to trust the systems that connect us, that enrich our lives economically and socially. And that means that cyber security matters to everyone. This year's Annual Review underlines this and shows how the NCSC, as part of GCHQ, contributes to the UK's safety and prosperity. At a time of serious global economic and security risk, the need to make the UK the safest place to live and do business online is ever more relevant. I continue to be impressed by the expertise and dedication of our talented team.

Looking at the big picture, it is clear the cyber security threat is diversifying and evolving. We are seeing more states with cyber capabilities and more non-state actors joining the mix. We are also experiencing a shift in technology leadership towards the East. These factors and more have implications for the cyber security threats we all face.

The past 12 months have reminded us that global events have a direct impact at home. President Putin's unprovoked war in Ukraine has involved a range of cyber activities that we, and partners, have attributed to Russia.

Ukraine's resistance to the illegal Russian invasion has been impressive, both on the battlefield and in cyberspace. It shows that online, the defender gets to choose how vulnerable they are to attack. And how greater cooperation between big tech companies and governments on security can make a difference. There are lessons here for us all.

In these challenging times, the UK's cyber power, alongside the more traditional forms of diplomacy and statecraft, will play a vital role in maintaining national security and prosperity. To enhance current defences, we must increase our efforts to ensure UK businesses and government improve levels of cyber resilience. We must continue to re-evaluate and reinvent cyber security to stay ahead.

And that's precisely what the NCSC is doing. This is about better understanding. For example, through the Cyber Aware campaign, the NCSC is arming individuals and organisations with the knowledge they need to stay safe online, including against ransomware attacks. It's also about actively reducing the threat, as the latest Active Cyber Defence service that the NCSC has brought online is doing. Early Warning is free and open to any organisation and it has already sent six million monthly alerts to its 7,500 and growing members to inform them of potential threats, risks and vulnerabilities on their networks so they can take action. By galvanising the cyber security community across the UK, the NCSC is driving a whole of society approach.

The global shifts we are witnessing will take decades to settle. Whilst I can't predict how things will turn out, I can confidently say that cyber and cyber security will continue to be pivotal to our nation's success. We are committed – in the NCSC and across the rest of GCHQ – to working tirelessly to ensure the country's cyber security will be equal to the challenges of tomorrow.

Sir Jeremy Fleming, Director GCHQ

NCSC CEO FOREWORD

I am proud to present the NCSC's Annual Review of 2022. As you will see, it has been a year of impressive achievement for the team I am really proud to lead, but also one in which the cyber security threat has evolved significantly.

The most profound change in the cyber security landscape over the past 12 months came with Russia's invasion of Ukraine. The return of war to Europe presented a unique set of challenges in cyberspace for the NCSC, our partners and our allies. We have been part of a huge effort to ensure UK organisations, critical infrastructure and the whole of society are as resilient as they can be.

As well as keeping the UK safe, I am proud of the role the NCSC played, in conjunction with FCDO, in supporting the Ukrainian authorities' staunch cyber defence in the face of Russian hostility. These efforts were shown to have been critical in protecting the Ukrainians against Russian cyber attacks and raising their general cyber resilience.

These new challenges were accompanied by other, more familiar threats. Ransomware remains the most acute threat that businesses and organisations in the UK face. These attacks have genuine real-world consequences and are a reminder to all organisations of the importance of taking the mitigation measures set out in our guidance.

Low-sophistication cyber crime also continues to be a scourge to the British public and organisations, but it is heartening to see a growing uptake in our services to protect against these threats. Sign-ups to our Early Warning service rose by over 90%, while the 6.5 million reports from the public to the Suspicious Email Reporting Service (SERS) this year shows that people are both becoming more cyber aware and contributing to our resilience. The NCSC, in conjunction with our law enforcement partners, is more resolute than ever in its determination to thwart cyber criminals.

We are making significant progress in bolstering the UK's resilience, stopping hundreds of thousands of attacks upstream while bolstering preparedness and helping UK institutions and organisations better understand the nature of cyber threats, risks and vulnerabilities downstream. Despite this, there remain serious gaps in the nation's defences, and the collective resilience-building effort must continue apace.

This Annual Review is as much about what lies ahead as it is about the current challenges. We highlight the threats on the horizon, including the growing commercial availability of malicious and disruptive cyber tools and the risk of those falling into the wrong hands. This contrasts with the positive technological insight that NCSC experts provide in support of the UK's values-driven approach to developing future technologies and the principles that underpin them. This work makes a global contribution and reflects the NCSC's efforts to innovate and build capability to ensure that the technology on which our economy and society depend is secure, resilient and reliable.

We also look at the opportunities to grow a strong, healthy and diverse cyber security ecosystem, one of the pillars of the National Cyber Strategy. This is critical for national security, is essential to maintaining the UK's global leadership in critical technologies and has a significant part to play in the growth of the UK economy. Working alongside government, academia and industry, the NCSC will continue building that ecosystem into the future.

Central to this is a diverse, talented workforce, and I am pleased to see that over the past 12 months initiatives such as CyberFirst have engaged thousands more bright, enthusiastic young people in cyber security. This is a source of great optimism as we move into 2023.

Lindy Cameron, CEO of the National Cyber Security Centre

THREATS, RISKS & VULNERABILITIES

One of the most important roles of the NCSC is to identify, monitor and analyse key cyber security threats, risks and vulnerabilities. This informs how the organisation, wider government and the whole of society can keep ahead of and respond to these challenges.

Over the past year, the cyber security threat to the UK has evolved significantly. The threat from ransomware was ever present – and remains a major challenge to businesses and public services in the UK. This year 18 ransomware incidents required a nationally coordinated response, including attacks on a supplier to NHS 111, and a water utility company, South Staffordshire Water.

The most significant threat facing citizens and small businesses continued to be from cyber crime, such as phishing, while hacking of social media accounts remained an issue. Official figures revealed there were 2.7m cyber-related frauds in the 12 months to March 2022 in the UK[1].

Internationally, Russia's invasion of Ukraine brought the cyber security threat into sharper focus in the UK. During the invasion, Russia sought to use offensive cyber operations to support their military campaign. However, like on the battlefield, Ukrainian authorities – assisted by the NCSC – created strong cyber defences, limiting the impact of Russian operations. Ukraine's successful defensive operations were an exemplar to network defenders across the world.

While not as prominent as Russian operations in cyberspace, the Chinese Government's cyber capabilities continued to develop. Beijing's activity has become ever more sophisticated, with the state increasingly targeting third-party technology and service supply chains, as well as exploiting software vulnerabilities. This approach shows no sign of abating, with China's technical evolution likely to be the single biggest factor affecting the UK's cyber security in the future.

Evolving state threats were not the only cyber security challenges this year: the proliferation and commercial availability of cyber capabilities continued and is likely to expand the threat to the UK. It is expected that further malicious and disruptive cyber tools will be available to a wider range of state and non-state actors, and will be deployed with greater frequency and less predictability.

Threats to the global supply chain continued to be apparent this year where attackers accessed target victim organisations' networks or systems via third-party vendors or suppliers. Meanwhile, the disclosure of the Log4j vulnerability highlighted the challenges where weaknesses in IT systems are exploited to deliver successful attacks.

In response to these notable threats the NCSC stepped up its automated notification service Early Warning, which was launched in May 2021. By the end of August 2022 34 million alerts were sent to its 7,500 and growing members to inform them of potential threats, risks, vulnerabilities or open ports in their networks.

While the NCSC sought to stop as many attacks getting through as possible – 2.1 million commodity campaigns were removed this year – it worked throughout with its partners to respond to incidents when they occurred, and helped victims to recover. This year the NCSC managed the response to hundreds of incidents, 63 of which were nationally significant.

1 https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022

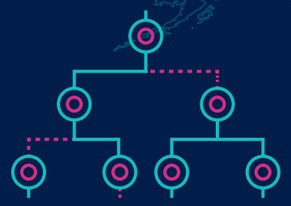
Threats, risks & vulnerabilities

Ransomware

A form of malware used by cyber criminals to prevent or limit users from accessing their systems or data – or threatening to leak it - until a ransom is paid

Commodity attacks

High-volume, low-sophistication attacks usually involving phishing and other scams often reaching citizens and small businesses



Proliferation

Increased commercial availability of high-end disruptive and offensive cyber capabilities and tools used by state and non-state actors

Supply chain

Attacks where perpetrators access an organisation's network or systems via third-party vendors or suppliers

Vulnerabilities

Weaknesses in an IT system that can be exploited by an attacker to deliver a successful attack

The threat from state actors

Russia

used cyber capabilities to maximise operational impact in Ukraine.
A seasoned cyber aggressor with a record of attacks against its neighbours and the UK, including attempts to steal Covid vaccine research in 2020

China

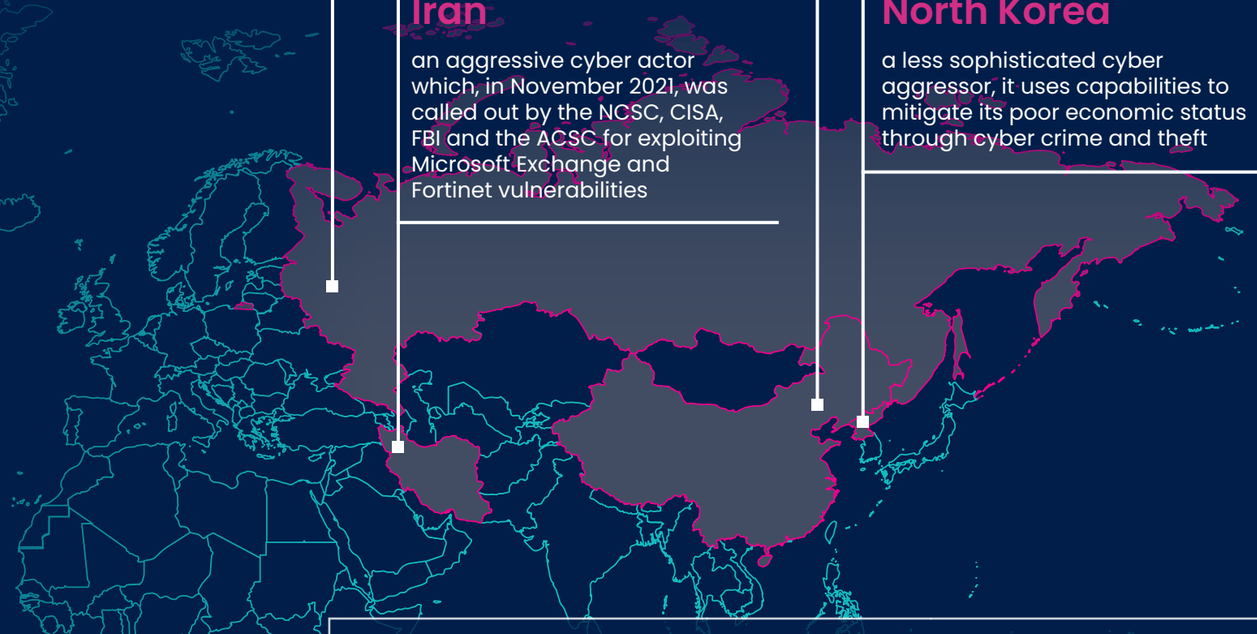
is becoming ever more sophisticated, increasingly targeting third-party technology, software and service supply chains

Iran

an aggressive cyber actor which, in November 2021, was called out by the NCSC, CISA, FBI and the ACSC for exploiting Microsoft Exchange and Fortinet vulnerabilities

North Korea

a less sophisticated cyber aggressor, it uses capabilities to mitigate its poor economic status through cyber crime and theft



State threat methods

The type of threats posed by these states varied widely, including:

- Disproportionate cyber-enabled espionage
- Reckless use of destructive cyber capabilities with the potential to cause harm to innocent victims
- Cyber-enabled theft of intellectual property or personal data of citizens for commercial advantage
- Undermining of legitimate democratic institutions including electoral processes

RESILIENCE

Building cyber resilience and maturity is fundamental to the UK's economic and national security interests. This means having strong cyber defences where most attacks are prevented or blunted, and the ability to prepare, respond, recover and learn when attacks get through.

To that end, the NCSC played a key role this year in helping UK institutions and organisations better understand the nature of cyber threats, risks and vulnerabilities, helping them to take action to secure the systems and services that society depends on; stopping attacks upstream and bolstering preparedness for when incidents occur to minimise the impact and recover more effectively.

As well as supporting organisations and institutions, the NCSC's resilience efforts also incorporated citizens, businesses, essential and critical services, government and public sector.

This "whole of society" approach is central to the government's new National Cyber Strategy (NCS), which was published in December. It set the ambition of "building a resilient and prosperous digital UK" and defined three areas of focus: managing risk, securing systems and being resilient.

As stated in the NCS "significant progress has been made in the last decade in improving our cyber resilience, with the establishment of the National Cyber Security Centre (NCSC), increased availability of advice, guidance and other tools, and the implementation of legislation… But serious gaps remain. Cyber breaches affect government, businesses, organisations and individuals; many organisations still report high numbers of cyber security breaches or attacks."

In addressing these challenges the NCSC continued to do all it could to stop attacks – 2.1 million malicious cyber campaigns were removed this year – and engage and equip sectors with new and updated advice, tools and services. And in partnership with the government and others continued to:

- monitor, assess and prioritise multiple threats and risks
- make the internet automatically safer, preventing attacks and building-in basic protections
- reduce the security burden on citizens, businesses and organisations, and doing more to protect those who are vulnerable
- secure systems to prevent and resist cyber attacks
- support the government in becoming an exemplar in cyber security
- support embedding cyber security in organisational risk management through use of regulation and other incentives
- harness the power of threat insight to build communities that can defend themselves

This year was a case of the "three Rs" of resilience: ransomware, Russia and renewal.

Ransomware

With ransomware continuing to be a significant threat the NCSC sought to increase resilience to this evolving form of malware through:

- alerting audiences about latest threats, risks and vulnerabilities and updating and clarifying advice and guidance on how to mitigate them
- engaging directly with sectors, especially those at risk, to encourage take-up of services, tools and behaviours, including webinars, roundtables, site visits and briefings
- widening the scope and refreshing its advice, guidance and services, including the renowned Active Cyber Defence programme

Russia

Weeks before Russia's invasion of Ukraine the NCSC moved to update its guidance and alert UK businesses, organisations and citizens about the actions to take in the event of a heightened cyber threat. New guidance explained in what circumstances the cyber threat might change and outlined the steps organisations should take in advance, which included fundamental protections of patching, backups, incident planning and system monitoring.

The NCSC worked closely with the FCDO to develop a strategy to support the Government of Ukraine, drawing on capabilities and its expertise and that of industry partners to bolster their defences. These efforts proved critical in protecting the Ukrainians against Russian cyber attacks, and raising their general cyber resilience.

Renewal

While ransomware and Russia attracted a particular focus this year, the NCSC pursued a "threat-informed" approach to its continued resilience-building across a wide range of sectors.

Earlier this year it was revealed that 39% of businesses in the UK had suffered a cyber attack over the previous 12 months, with many facing a material outcome, such as loss of money or data[2].

The NCSC's resilience efforts included a continual cycle of engagement and support, in the form of webinars, briefings, bulletins and workshops, to inform and alert sectors of threats, risks and vulnerabilities, while showcasing and signposting them to refreshed advice, guidance, tools and services, giving them agency to apply these resources to help improve their resilience.

Reducing the burden

At the same time, engagement continued with technology and digital service providers to make the internet and connected services and devices more secure at source and behind the scenes, reducing the burden on end-users.

Resilience at scale

One of the NCSC's cornerstone programmes, Active Cyber Defence, continued to play an important role in bolstering resilience this year. Notably, since its launch in April 2020 the Suspicious Email Reporting Service (SERS) has received 13.7 million reports, resulting in the take down of 174,000 scam URLs.

In April the NCSC opened up its Web Check and Mail Check services to the whole education sector to better protect schools, colleges and universities from cyber attacks. At the year's end there had been a 42% increase in users of the Exercise in a Box service; a 37% increase in users of Web Check; 46% decrease in fake government scams; and a 23% rise in the number of organisations using PDNS.

Resilience assured

One of the most recognised assurance schemes is Cyber Essentials, which helps organisations assess and manage their own cyber risks. This year 28,989 certificates were awarded, including 5,799 businesses achieving Cyber Essentials Plus status. After having received a major upgrade in January, the scheme achieved a key milestone in July when it reached 100,000 certificates issued since it was first launched.

2 https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

Resilience highlights this year

2.1 million
cyber-enabled commodity campaigns removed

6.5 million
suspicious email reports received & 62k scam URLs removed

34 million
Early Warning alerts about attacks, compromises, vulnerabilities or open ports

90%
increase in signups to Early Warning service.

Expansion
of counter-ransomware services

Support to Ukraine
in bolstering their cyber resilience in the face of Russian invasion

Bolstered UK resilience
in light of heightened cyber risk from the conflict

UK-wide Cyber Aware campaign
to change citizen behaviour around personal email security

CYBER ESSENTIALS

15% rise in certificates awarded (28,989)

5,799 businesses achieved "Plus" status – a **15%** increase on last year

Now over **300** cyber security companies licensed as certification bodies for Cyber Essentials

Cyber Essentials-certified SMEs **60%** less likely to need to make a cyber insurance claim

100,000th Cyber Essentials certificate issued (since launch)

Active Cyber Defence

Protective Domain Name Service (PDNS) - prevents users from accessing malicious domains or IP addresses.

- Organisations using PDNS rose **23%** (from 928 to 1,140)

Mail Check helps public and third sector assess and improve email security compliance to prevent criminals spoofing email domains.

- New users increased by 43% (from 1,386 to 2,448)
- **Domain-based Message Authentication, Reporting and Conformance** (DMARC) protection in place has increased:
  - From 58% to 68% of public sector organisations
  - From 21% to 29% Universities
  - From 21% to 27% further education colleges
  - From 11% to 16% of the top 3,000 charities

Exercise in a Box (EiaB) - a toolkit of scenarios for organisations to refine their response to cyber security incidents.

- New users increased by 42% (from 11,851 to **16,808**)

Early Warning Service - a free service to notify members about potential attacks , compromises, vulnerabilities or open ports on their networks.

- Over 90% increase in signups this year (from 3,924 to 7,523)
- 34 million notifications issued about potential threats, risks, vulnerabilities or open ports in user's networks

Email Security Check - free for all UK organisations to check for correctly applied standards like DMARC and Transport Layer Security (TLS)

- Since launch in April 2022 the service has been used for **32,000 checks**

Vulnerability Disclosure Services - to report, manage and remediate vulnerabilities in government and other key services

- **Over 750 reported** vulnerabilities across the UK government remediated

Suspicious Email Reporting Service (SERS) allows the public to report potential scam messages for removal.

- Reports increased by 20% going from 5.4m to 6.5m
- Total number of reports reached 13.7m (since April 2020)
- 62k scam URLs removed, bringing total takedowns since SERS started to 174k

Takedown Service - works with hosts to remove malicious sites and infrastructure from the internet.

- Share of global phishing remained at 2%, in 2016 the figure was over 5%
- Number of fake UK government phishing scams decreased by 46% (from 13,000 to 6,000)
- 2.1 million cyber-enabled commodity campaigns removed

Web Check - helps users find and fix common security vulnerabilities in their websites.

- New users increased by 37% (from 3,539 to 4,849)
- 43% increase in unique URLs scanned using Web Check
- 12.5% increase in urgent findings reported to users, along with remediation advice

TECHNOLOGY

This year the NCSC continued to develop insights, capabilities and principles to help ensure critical technology is secure, resilient and reliable in order to protect data, devices and services that underpin the wider UK digital economy, while preserving the values of a free and open cyberspace.

From the development of blogs and research papers that informed new legislation, regulation or codes of practice, to creating tools and guidance that monitored, identified or fixed vulnerabilities, the NCSC continued to innovate and build capability, while influencing those around it to further the UK's cyber security interests.

This year the NCSC saw the dependence of society on technology continue to grow and become more embedded in the daily lives of citizens, businesses and essential services.

Technology continued to be the subject of geopolitical competition between states who see, and begin to realise, the opportunities of technological advantage. As this competition grows, the UK faces an increasingly fragmented technology ecosystem which creates risks for interoperability and the values that underpin it.

Over the past year, the NCSC continued to track and assess the implications and risks of key areas of competition:

- **Technology standards -** where states such as China seek to supplant the originating, founding principles of privacy and security that underpin today's technologies. Through its "standards strategy", including filling key positions on Standards Developments Organisations (SDOs) and other international forums, and its proposals of a "top-down" and "centralised control" approach for the design of the future internet, China is seeking to implant its authoritarian traits of surveillance and control into tomorrow's technologies.

- **Digital dependence -** the debate over Huawei and its role in the UK's 5G networks prompted governments around the world to understand they were facing potential national security risks through their dependence on technology from countries with authoritarian regimes. Governments continue to assess their CNI supply chains and seek to mitigate the risks by removing or restricting technologies from the countries they distrust. This is hastening the partition of technology into an ecosystem dominated by the "West" and an eco-system dominated by China. Related to this issue are the implications of China's *Digital Silk Road* initiative where third-party states are dependent on Beijing in developing their digital infrastructure.

Fragmentation

The combined effect of changes in standards and the split into multiple ecosystems has led commentators to talk of the worsening bifurcation, or fragmentation, of the internet. While the internet, due to its decentralised evolution, has always been fragmented to a certain extent, what linked it together was its levels of interoperability. Although the overall impact of this more harmful fragmentation is still unclear it is likely it will have far-reaching consequences. By way of example, in the past, European travellers couldn't use their mobile phones in the United States as they wouldn't work. Society could be heading back to that sort of divide where users on each side would not be able to communicate with the other. And if they did, they might need to do so at the cost of privacy, security or functionality.

In response to these and other big challenges, the NCSC is supporting the UK Government in shaping the country's future technology and communications systems and dependencies, and limiting reliance on suppliers or technologies that are developed under authoritarian regimes.

In helping to address this, the NCSC stresses the importance of:

- increasing co-operation and co-ordination between allies to promote and instil shared values into the design and development of technologies societies depend on

- supporting a multi-stakeholder approach to standards development, ensuring standards encode democratic rather than authoritarian values

- increasing the diversity and resilience of critical supply chains so they can withstand shocks and adversarial interference

- continuing to investin foundational science, research and development, and early-stage industrialisation, and ensuring this research is protected from hostile activity

- investing in and building technology that upholds the UK's values and ethical approach to privacy, safety and security.

As well as providing insight, evidence and expertise to support a values-driven approach to the development of future technologies, the NCSC continued to innovate and build capability to help keep up and ahead of the ever-evolving threats, risks and vulnerabilities described earlier. Overleaf, is a snapshot of the avowed technical work of the NCSC.

Technology – A year of innovation and capability-building

- Developed and delivered a **tool to discover new mobile network vulnerabilities** and improve security for users
- Jointly **developed National Telecoms Signal Monitoring Service** (NTSMS) to improve understanding of threat and defences

- Supported development of UK's **Electronic Communications (Security Measures) and related draft Code of Practice**
- Welcomed launch of **Product Security and Telecommunications Infrastructure Bill** to strengthen cyber security for consumer devices and accountability of manufacturers

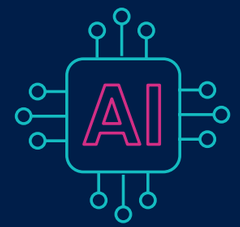
- Launched **Device Security Principles for Manufacturers** to help protect Enterprise Connected Devices from common threats and risks
- Updated all **cloud guidance** to reflect how much these services have changed in the past decade

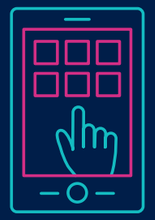
- Delivered **guidance to help small businesses** better understand technology risks such as 'Bringing Your Own Device' approaches and best practice for backing up data
- Refined **Cyber Aware advice** for citizens and microbusinesses focussing on email protection by using three random word passwords and two-step verification

As well as providing insight to support a values-driven approach to the development of future technologies, the NCSC continued to innovate and build capability to help keep the UK the safest place to live and work online.

- Published research papers and blogs including on zero trust for customers looking to begin a migration journey to zero trust architecture

- Supported **development of HMG's artificial intelligence strategy;** and continued to research opportunities, threats and ethics around AI
- Issued guidance in the form of **principles for artificial intelligence** (AI) and machine learning (ML) systems





- **Notified Google of fifteen suspicious applications**, that could have undermined users' security, resulting in the majority being taken down
- Worked with DCMS to provide technical input on the **Code of Practice for App Privacy and Security**, which will be a world-first when published.

- Guidance to help companies implement **vulnerability disclosure processes;** also published by the international standardisation body, ETSI
- Held two conferences (Safety, Security and Verification in Critical Systems and VICECon) focused on **bringing experts together** on topics around vulnerability research and knowledge sharing

ECOSYSTEM

The NCSC has a key role in strengthening the UK's thriving cyber security ecosystem, which is now worth more than £10 billion to the economy, employing nearly 53,000 people across 1,800 businesses.

Together with the Department for Digital, Culture, Media and Sport (DCMS), the UK Cyber Security Council (UKCSC) and other partners, the NCSC is creating an ecosystem that is self-sustaining and continues to be an essential part of the country's national security and economic interests.

From nurturing young talent, to creating further education opportunities, to supporting cyber startups, to testing and certifying standards, to creating more diversity, to driving growth and innovation, to sharing best practice with the industry, the NCSC is making a positive difference across the ecosystem.

In February, analysis revealed record levels of growth in the UK's cyber security sector with a 24% and 13% increase in new businesses and jobs respectively. The NCSC has been a part of this growth through its shared ambition, investment, dedication and collaboration with government, academia and industry. This has helped to create a dynamic and respected sector with a highly skilled and motivated workforce.

However, it is evident the sector faces challenges when it comes to optimising growth, skills and diversity. Too many vacancies go unfilled, while the workforce doesn't always reflect the diversity of wider society.

The second joint NCSC-KPMG Decrypting Diversity survey, published in December, reported many positive developments in equality and diversity within the sector, but further improvements were highlighted to increase inclusivity in many areas, such as gender, sexual orientation, ethnicity and social mobility.

Through developing a diverse and technically skilled workforce, harnessing the innovative talents of the UK's vibrant research community, and supporting a cyber resilient and innovative cyber sector, the NCSC's projects and initiatives are fortifying the UK's defences and creating a world-class cyber ecosystem.

Finding talent

The NCSC's **CyberFirst** programme, which provides opportunities for young people to get into cyber security, saw more than 7,000 girls take part in this year's Girls Competition. 130 teams from across the UK reached 13 regional and national finals in February with a winner crowned at each. 50,000 girls have now taken part in the competition since 2017.

The **CyberFirst Schools & Colleges scheme** saw eight more schools and colleges receive a CyberFirst schools award for "first-rate technology and cyber security teaching". Since the initiative launched in 2020, 57 schools and colleges have attained CyberFirst recognition for helping to develop cyber ecosystems around the country.

Nurturing talent

For Higher Education the number of certified **Academic Centres of Excellence in Cyber Security Education** grew to 13 this year, while 21 more degree course were certified by the NCSC.

The **CyberFirst Bursary** programme continues to support the next generation of cyber talent, providing a £4,000 bursary and paid cyber security training each summer to undergraduates. This year, 85 students were offered new bursaries with 42% being female candidates.

Realising talent

The **NCSC for Startups** initiative continued to translate talent into jobs, opportunities and growth this year. This project brings government and industry together to develop, adapt and pilot technology to meet the biggest cyber security challenges facing the UK. Over the past year, 14 new organisations were onboarded to the initiative, taking the total number of participants to 62 since the scheme started in 2017. Alumni have now raised over £420million in funding and have created over 700 new roles.

In March, 50 undergraduates and postgraduates studying NCSC-certified degrees took part in the first-ever **Innovators Challenge.** The three-day event in Manchester tasked the students with working in teams to find innovative solutions to two cyber security challenges facing the UK – securing the supply chain and safe remote working.

Assuring talent

A key focus of the ecosystem development work is the NCSC assurance and certification schemes for industry. This year the **NCSC relaunched schemes** such as **Cyber Incident Response**, while introducing new ones to broaden the market and allow a wider cross section of industry to work with the NCSC or find support from it.

Applying talent

In July, the NCSC launched its new **Cyber Advisor scheme** by funding 100 assessments of potential participants which checked whether they possessed a good understanding of baseline security controls and had the ability to provide practical help to companies which want to meet certain standards. As well as launching Cyber Advisor, the NCSC refreshed the **Assured Cyber Security Consultancy** scheme, and developed a new standard, assessment criteria and process.

Since the formation of the UK Cyber Security Council, the industry body for the cyber security profession, the NCSC has worked closely with them on a range of shared challenges. In one key area, the NCSC has been working to pass the stewardship of the **Certified Cyber Professional scheme** to UKCSC.

The NCSC has been broadening its **Cyber Incident Response (CIR)** scheme to support government, CNI and large corporate organisations in their preparedness for significant targeted cyber attacks. This included rewriting the Technical Standard and new application process for the Cyber Incident Response scheme. Meanwhile, a Cyber Incident Exercising pilot was successfully completed in partnership with the NCSC Exercising Team and industry.

Sharing talent

The NCSC's long-standing **i100 (Industry 100) scheme** continued to foster collaboration between public and private sector through placements of industry professionals within the organisation. Now in its fifth year, the scheme has seconded 180 industry partners into teams across all areas of the NCSC, with 39 new participants taking up the opportunities in the last 12 months.

UK's cyber security sector at a glance

Value

£10.1 billion[3] (up 13.4%)

Employers

1,838 cyber security companies (up 24%)

Jobs

52,700 (full-time equivalents) people employed (up 13%)

Investment

>£1 billion raised across **84** deals

Nurturing talent

CyberFirst Girls Competition 2022

More than
7,000
girls entered

130 teams
with
13
regional and national finals

85% of schools
participating in the Girls Competition are state run

50,000 girls
have taken part in the competition since 2017

CyberFirst Bursary

85 students
joined CyberFirst bursary scheme

42%
were female and
23%
from ethnic minority backgrounds

Total number of bursary students reached
1,000

93%
of whom are now in cyber security roles

Recognising Schools, Colleges and Universities

Eight more schools and colleges received CyberFirst status, taking total to 57

18 postgraduate, three undergraduate and two graduate degrees certified taking total to **63** throughout the UK

>33% of universities now offer NCSC-certified postgraduate degrees in cyber security

13 universities formally recognised for offering first-rate cyber security education

First ever Innovators Challenge this year, with **50** students taking part

3 DCMS Cyber Security Sectoral Analysis 2022

Supporting the industry

Employee headcounts at NCSC for Startups-backed firms went **from 475 to 1,210 across 62 enterprises**

Investment in NCSC for Startups-backed firms went from £100 million to **£422 million**

Stewardship of the Certified Cyber Professional scheme passed to UK Cyber Security Council

39 new participants joined the i100 scheme

CYBERUK 2022

The UK's flagship cyber security event brought together the ecosystem in Newport, Wales, in a two-day conference that saw:

Event facts

2,230 in-person delegates

16,318 YouTube views

170 speakers across **31** sessions and **14** workshops

25 sponsors, **119** exhibitors over **6,400** sqm of space

Delegate feedback

92% rated the event as good/excellent

85% report it will help to protect their organisation online

85% claim their knowledge has increased as a result of attending

85% say they made three or more new contacts as a result of attending

Report suspicious emails
to **report@phishing.gov.uk**

Report suspicious websites
via **ncsc.gov.uk**

Report suspicious text messages
to **7726**

National Cyber Security Centre
a part of GCHQ

GCHQ

This is an executive summary, with the full version available at **ncsc.gov.uk/annual-review-2022**

@NCSC

National Cyber Security Centre

@cyberhq

To request the information in this document in an alternative format please email **enquiries@ncsc.gov.uk**

Designed and created by Agent Marketing Ltd. **helloagent.co.uk**

FSC
www.fsc.org
MIX
Paper from responsible sources
FSC® C113965