
${jndi:ldap://example.com:1234/callback}
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.

TIMELINE

10 September

Top cyber security officials from the UK and US affirm their commitment to tackling ransomware

29 September

National Cyber Awards recognise NCSC Director of Operations, Paul Chichester as 'Cyber citizen of the year'

6 October

NCSC recognise three more universities for showing commitment to delivering first-rate cyber security education on campus and beyond

18 November

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

23 November

NCSC and KPMG publish the 2nd Decrypting Diversity report, hosting an event to reflect on progress and challenges in the cyber security industry's diversity ambitions

26 November

NCSC Cyber Aware campaign launch encouraged citizens to secure their email and to report suspicious texts, emails and websites, during the online shopping peak of Black Friday and Cyber Monday

6 December

NCSC for Startups welcome four more innovators, who will develop, adapt and pilot technology to solve some of the UK's most important cyber challenges

10 December

Patching and monitoring advice issued to mitigate Apache Log4j vulnerabilities

15 December

Government's National Cyber Strategy published, calling on all of society to play their part in reinforcing the UK's economic and strategic strengths in cyberspace

17 January

Guidance issued for organisations on the heightened cyber threat, considering Russia's invasion of Ukraine

24 January

Cyber Essentials scheme refresh, including revisions to the use of cloud services, home working, multi-factor authentication, password management, and security updates

28 January

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

2 February

NCSC join the seL4 Foundation

7 February

A new-look CyberFirst Girls Competition crown its competition winners – after teams of 12-13-year-olds took on challenges covering topics from networking and AI to cryptography and logic

9 February

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

18 February

The UK Government assess Russia to have been involved in DDoS attacks on Ukraine

21 February

Lindy Cameron urges UK organisations to strengthen their cyber defences during times of heightened alert

18 March

Members of the public report over 10.5 million suspicious emails, resulting in the take down of 76,000 online scams. This news was accompanied by a new national Cyber Aware campaign, endorsed by the Home Secretary and Chancellor of the Duchy of Lancaster

18 March

Following Russia's attack on Ukraine, the NCSC provide a list of actions for organisations in the UK to implement to bolster their online defences

31 March

Director GCHQ Sir Jeremy Fleming gives speech on global security amid the war in Ukraine, in a speech delivered at the Australian National University, Canberra

10 May

UK and US attribute a series of cyber attacks to Russia against Ukraine in the hours before the invasion

10 May

NCSC's Active Cyber Defence programme publishes its fifth report

10-11 May

CYBERUK22 in Wales, Newport. New service Mail Check 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 emphasises the importance of partnerships and international regulation of sophisticated cyber capabilities

8 July

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

25 July

A new Cyber Advisor Pilot scheme announced

23 August

Construction firms working together on major building projects such as HS2 offered bespoke advice aimed at helping firms keep sensitive data safe from attackers

DIRECTOR GCHQ

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 co-operation 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 is 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, like 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 act. 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 cannot 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

CEO NCSC

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 highly successful 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 important 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) 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 depends 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

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

CHAPTER 1 - THREATS, RISKS AND VULNERABILITIES

Introduction

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

Over the last 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 co-ordinated 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.

Internationally, Russia's invasion of Ukraine brought the cyber security threat into sharper focus in the UK. During the invasion, Russia sought to use disruptive 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 was an exemplar to network defenders across the world.

While not as prominent as Russian operations in cyberspace, the Chinese state's cyber capabilities continued to develop. China'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 where attackers accessed target victim organisation's 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 with the launch of Early Warning, in May. One of the newest ACD services, Early Warning, which is free and open to any organisation, had, by the end of August 2022 sent 34 million notifications to its 7,500 and growing members to inform them of potential threats, risks, vulnerabilities or open ports in their networks. This included alerting them to over 500 unique malware variants.

While the NCSC sought to stop as many attacks as possible getting through – 2.1 million commodity campaigns were removed this year – it worked throughout 2022 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.

This chapter sets out the key threats, risks and vulnerabilities in more detail and the NCSC's analysis and response.

State threats

The UK is a responsible, democratic cyber power that seeks to maintain its competitive edge in the rapidly developing cyber domain and uses the UK's full spectrum of levers to detect, disrupt and deter its adversaries. However, there are some state actors, with malign intent, that do not operate under the same legal and democratic framework. Over the last year, the NCSC has continued to see state actors present a significant threat towards the UK and global cyber security. This is supported by the National Crime Agency's (NCA) intelligence and threat assessments.

While many countries use malign cyber capabilities to some extent, including to control their domestic information environments, the regimes that continued to present the most acute cyber threat to the UK and its interests were Russia, China, Iran and North Korea.

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

- Cyber-enabled espionage - unauthorised access or transfer of secret, classified or sensitive information to gain advantage over rivals
- Destructive cyber capabilities – using tools such as wiper malware to damage IT systems or institutions
- Cyber-enabled theft to further strategic advantage or domestic control, for example of Intellectual Property or personal data of citizens
- Hack and leak – stealing and publishing sensitive or restricted information to embarrass states or institutions or to undermine social cohesion

These actions are used to target the local and national Governments of other states and their critical national infrastructure, institutions and internal political processes.

In the coming years, with the proliferation of commercially available capabilities, the NCSC anticipates a wider number of states possessing the ability to pose threats to the UK's cyber security.

Russia

The most significant development in the cyber security threat internationally was Russia's illegal invasion of Ukraine and their use of cyber operations within it.

Since its creation in 2016 the NCSC has viewed Russia's cyber capabilities and intentions as an acute and persistent threat to the UK's interests – and this year was no different. Russia's intelligence services are malign actors in cyberspace and have advanced cyber capabilities

which they use to target their adversaries, including Western institutions. The UK Government has attributed cyber activity to all three Russian intelligence services, these are:

- The GRU: Military intelligence
- The SVR: Foreign Intelligence Service
- The FSB: Federal Security Service

In the last year, this threat was underlined by Russia's invasion of Ukraine – a conflict in which they sought to use cyber capabilities to maximise their operational impact.

As Jeremy Fleming, Director of GCHQ, wrote in March: "*we have seen the Russian state try to align and co-ordinate cyber capabilities alongside more traditional facets of military power. To date, this hybrid intent has not succeeded; the impact has been less than we (and they) expected. In part, this is because Ukraine has proved itself to be an extremely effective cyber defender. Since the annexation of Crimea in 2014, it has painstakingly developed a digital fortress.*"[1]

In many ways, the first shots fired in the Russian invasion of Ukraine in 2022 were in cyberspace. A month before the Russian invasion, the GRU deployed *WhisperGate* wiper malware against Ukrainian Government targets. As the invasion drew closer, they launched Distributed Denial of Service (DDoS) attacks against Ukrainian Government websites[2] and in the hours before the invasion, conducted a cyber attack against ViaSat, the communications company. The aim of the ViaSat attack was to impact Ukrainian military targets, but it also disrupted other customers, including personal and commercial internet users.[3]

While UK organisations did not experience significant cyber impact resulting from Russia's invasion of Ukraine, Russia continues to be a persistent and active threat to the UK and its interests, which is why the NCSC continues to advise against complacency. In response to recent setbacks Russia has experienced on the battlefield in Ukraine, they could change their approach in the cyber domain of the conflict. The NCSC continues to recommend organisations follow its advice on operating in periods of heightened tensions[4].

The Russian cyber activities seen in Ukraine are the most recent examples of Russian activity in cyberspace, including against the UK. In recent years, the NCSC has called out the Russian State for its involvement in the compromise of SolarWinds, targeting the COVID vaccine supply chain and destructive cyber attacks against Georgia and Ukraine. In the last year, the NCSC published a technical advisory highlighting new malware used by the Russian GRU's Main Centre for Special Technologies – often known as "Sandworm" – the group behind the NotPetya attacks in 2017[5]

---

[1] From Jeremy's Economist piece.

[2] https://www.ncsc.gov.uk/news/russia-ddos-involvement-in-ukraine

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

[4] https://www.ncsc.gov.uk/section/keep-up-to-date/heightened-threat

[5] https://www.ncsc.gov.uk/news/joint-advisory-shows-new-sandworm-malware-cyclops-blink-replaces-vpnfilter

China

As the Government's Integrated Review and National Cyber Strategy made clear, China's technical development and evolution is likely to be the single biggest factor affecting the UK's cyber security in the years to come.

China has also identified several existing and emerging technologies as being vital to its future national security. It has directed significant resources into emerging tech research and development and continues to push not only for parity with Western countries, but for technical supremacy. The technologies that China seeks to achieve dominance in include artificial intelligence (AI), quantum computing and semiconductors.

Since taking power nearly a decade ago, President Xi has overseen extensive reform of China's intelligence and military apparatus, with a key priority being the fusion of military and civilian cyber capabilities. Since then, China's Ministry of State Security (MSS) has emerged as a prolific and pervasive actor in cyberspace, undertaking a substantial global espionage campaign to meet political, socio-economic, and strategic objectives.

Following reforms, there has been a notable increase in the operational security, sophistication and ambition of both the MSS and the People's Liberation Army (PLA). Electronic warfare, cyber and space capabilities have been consolidated into a single structure to enhance the military's cyber power and information operations capabilities.

The Chinese cyber forces are also by far the largest in the world. In April 2022, FBI Director Christopher Wray judged that China has "a bigger hacking program than that of every other major nation combined[6]

The global scale of activity from these organisations has been well documented and the UK Government has called out various examples of malign Chinese behaviour in cyberspace, including the compromise of thousands of enterprises' Exchange servers around the world, through exploitation of a zero-day vulnerability.

Chinese activity has become ever more sophisticated, with China increasingly targeting third-party technology and service supply chains, as well as successfully exploiting software vulnerabilities. This approach shows no sign of abating.

Iran

The threat of cyber activity by the Iranian State first came to prominence in 2011, when it launched a campaign of DDoS attacks against the US financial sector, which continued into 2013[7]. Using this relatively unsophisticated method, Iran was able to inflict damage which cost tens of millions of dollars to mitigate.

Iran remains an aggressive cyber actor with a range of espionage, disruptive and destructive cyber capabilities. Cyber actors associated with the Iranian State have also been implicated in attacks against victims in many countries. An example of this approach in the last year has been Iran's attacks against the Government of Albania, which the UK Government recently

---

[6] https://www.cbsnews.com/news/fbi-director-christopher-wray-60-minutes-2022-04-24/

[7] https://www.fbi.gov/news/stories/iranians-charged-with-hacking-us-financial-sector

called out[8]. This attack involved the destruction of Government data and the disruption of essential government services, including in healthcare and education.

Although Iranian cyber actors' capabilities are thought to be always improving, they rarely use the most advanced or up-to-date capabilities to conduct their operations. Iranian actors do not rely on zero-day vulnerabilities (recently discovered vulnerabilities that are not yet publicly known), as they have had success using published vulnerabilities to gain access to unpatched systems.

In November 2021, the NCSC joined the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) in the US and the Australian Cyber Security Centre (ACSC) to highlight that an Iranian state backed group were exploiting Microsoft Exchange and Fortinet vulnerabilities, with the NCA's National Cyber Crime Unit (NCCU) coordinating the law enforcement response to the compromise.[9]

North Korea (DPRK)

While not as sophisticated as Russia, China and Iran, North Korea (DPRK) remains a capable actor in cyberspace. A key focus of North Korea's malign cyber activity is cyber theft, using its cyber capability to bolster its poor economic situation through cyber crime. It also uses cyber activity to further consolidate the current regime, and to strengthen and maintain the DPRK's ability to defend itself against perceived hostile actors.

Cyber crime

The UK is exposed to a wide variety of cyber crime threats – from those that have the potential to be national security threats, such as ransomware, to commodity cyber crime campaigns (attacks that use readily available tools that require little or no customisation) which seek to defraud the UK public and businesses.

Low sophistication cyber crime:

The cyber security threat that most of the British public are likely to experience is low sophistication cyber crime. Cyber criminals deploy commodity attacks, such as phishing or malware with the aim of scamming the public and businesses.

Phishing emails continue to be a successful attack vector for criminals. In many cases, these attacks are designed to mimic those online services that people use and often trust. In the last year, COVID-19 and the Russian invasion of Ukraine were prominent themes that criminals used to lure the public.

More recently, cyber criminals used the energy regulator Ofgem as a lure for over 50 phishing campaigns used to harvest financial credentials in response to rising energy costs. To mitigate this specific threat Ofgem wrote to all energy supplier CEOs asking they have clear, up-to-date and accessible information on their websites advising customers what to do in case of a scam.

---

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

[9] https://www.ncsc.gov.uk/news/microsoft-exchange-fortinet-vulnerabilities

Hacking of social media and email accounts, to financially extort victims for access to their accounts, or to compromise data to commit or enable fraud offences, has also grown over the past year. In 2021/22, there were a total of 8,023 reports of social media hacking, an increase of 23.5% on the previous year[10].

Ransomware

Ransomware is one of the most significant cyber security threats facing businesses and organisations in the UK. When ransomware is successfully deployed, it has the potential to prevent public services and businesses operating and put their data at significant risk.

What is ransomware?

- Ransomware is a type of malware which prevents users from accessing their device or network and the data stored on them, usually by encrypting files.
- A criminal group will then demand a ransom in exchange for decryption.
- The computer itself may become locked, or the data on it might be encrypted, stolen or deleted.
- The attackers may also threaten to leak the data they steal.

How does ransomware work?

- **Access**: Attackers gain access to victim's network. They establish control and plant malicious encryption software. They may also take copies of data and threaten to leak it.
- **Activation**: The malware is activated, locking devices and causing the data across the network to be encrypted, meaning it can no longer be accessed.
- **Ransom demand**: Usually victims will then receive an on-screen notification from the cyber criminal, explaining the ransom and how to make the payment to unlock the computer or regain access to data. Payment is usually demanded via an anonymous web page and usually in a cryptocurrency, such as Bitcoin.

For this reason, it is important to always have a recent offline backup of the most important files and data. Visit www.ncsc.gov.uk/ransomware on advice and tools

During the last year, the NCSC co-ordinated the national response to 18 ransomware attacks including the attacks on a supplier to NHS 111, and South Staffordshire Water. But the true numbers of ransomware attacks in the UK each year are far higher, as organisations often do not report the compromises.

[10] NFIB Cyber Annual Assessment 2021-2022

Last year, the NCSC joined forces with the FBI, CISA, the National Security Agency (NSA) and the ACSC to highlight that there had been an increase in sophisticated, high-impact ransomware incidents against critical infrastructure organisations globally[11]. Given its potential impact on critical national infrastructure and essential services, ransomware is considered a national security risk.

Ransomware is an illicit commercial enterprise: a threat that continues to evolve as the criminals behind it pursue the best ways to make money. In earlier years, the threat from ransomware was principally that criminals were able to block organisations accessing their systems through encryption. Increasingly the NCSC is seeing data extortion as a fundamental part of the ransomware business model, as criminals realise that many organisations are willing to pay to avoid their data being leaked.

Law enforcement does not encourage, endorse nor condone the payment of ransom demands. If you do pay the ransom:

- there is no guarantee that victims will get access to their data or computer;
- computer or networks will still be infected;
- criminal groups continue to be financed;
- Increased likelihood of being targeted in future.

This year, Lindy Cameron, CEO of the NCSC, wrote jointly with the Information Commissioner, John Edwards, to the Law Society and Bar Council. The letter made clear NCSC advice that payment of a ransom incentivises harmful behaviour by malicious actors and does not guarantee decryption of networks or return of stolen data, and the ICO position that payment of a ransom will not reduce any penalties incurred through their enforcement action.

The NCSC continued to see increased use of Ransomware as a Service (RaaS) where ransomware variants are leased to less-skilled affiliates who can launch cyber attacks without building the ransomware themselves. This opens the ransomware attack vector to a wider range of criminal actors where previously it was restricted to those with the requisite technical expertise.

In May 2022, it was reported that the Conti ransomware strain was discontinued. However, by August of that year it had not led to a reduction in the threat of ransomware to the UK as some members of the organised crime group behind it moved to other ransomware groups, meaning the NCSC is expecting to see a more diverse and capable ransomware landscape.

Most of the ransomware criminal groups that target the UK continue to be based in and around Russia. While it is not clear the degree to which these ransomware groups are directed by the Kremlin, those operating from within Russia's borders benefit from the tacit consent of the Russian State.

[11] https://www.ncsc.gov.uk/news/joint-advisory-highlights-increased-globalised-threat-of-ransomware

Cyber incidents in the UK

Over the last year, businesses and organisations in the UK reported hundreds of cyber incidents to the NCSC, 63 of which were significant enough to require a national level response. The incidents included a range of malicious cyber activity such as ransomware, reconnaissance, malware and network intrusions, data exfiltration and disruption of services and systems.

While the NCSC sought to stop as many attacks as possible getting through – 2.1 million commodity campaigns were removed – it worked throughout the year with its partners, including with the NCA to form a whole system approach, to respond to incidents when they occurred, and helped victims to recover.

Over the last year, the commercial cyber incident response sector has continued to mature. End to end support packages provided through cyber insurance policies, including legal assistance and technical response from cyber incident response companies, are becoming more common.

The NCSC's Cyber Incident Response (CIR) Level 1 scheme assures companies which deal with sophisticated, targeted attacks against networks of national significance. In the coming year the NCSC is planning to widen this out to include a Level 2 scheme which will provide technical response for incidents affecting small to medium-sized enterprises who require more accessible CIR support.

Although ransomware disrupted critical national infrastructure organisations last year[12] following a series of high-profile incidents, such as the attack against Colonial Pipeline in the US, it is apparent that the public outcry and heightened political interest has raised the stakes for cyber criminals. In response it became clear that some groups modified their techniques to avoid law enforcement, sanctions and other operational responses.

Evolving Technical Threat

Last year saw the response to the Log4J vulnerability which showed how widespread some low-level software flaws can be, how hard it is to know what underlying software libraries are in use in users' applications, and how quickly a vulnerability can be weaponised.

The Log4J vulnerability was made public in December and within days it was being exploited. Less than four weeks after it was made public, NHS Digital saw widespread targeting of the specific vulnerability in the VMware Horizon product13. The NCSC published alerts and guidance to highlight the risk posed by Log4J and mitigations. However, as the logging utility is widely used, there remains a significant risk where its vulnerabilities remain unpatched.

More generally, technical threat evolved at all levels of sophistication – not only at the "top" end. Activity attributed by Microsoft to NOBELIUM14 is an example of the evolution of highly technically sophisticated tradecraft.

---

[12] https://www.ncsc.gov.uk/news/joint-advisory-highlights-increased-globalised-threat-of-ransomware

[13] https://digital.nhs.uk/cyber-alerts/2022/cc-4002

[14] https://www.microsoft.com/security/blog/2022/08/24/magicweb-nobeliums-post-compromise-trick-to-authenticate-as-anyone/

The NCSC are also seeing changes in less sophisticated attacks – such as the increasing trend to use Multi-Factor Authentication (MFA) Push Exhaustion attacks. This sees attackers trigger a deluge of MFA acceptance prompts on a user's phone until the user clicks 'Allow' to stop the flood of requests. The ongoing attacker tendency of 'Living off the Land' – where the malign actor uses built-in software and functions to perform actions on target systems – means that activity by sophisticated actors can appear very similar to activity by unsophisticated ones.

Another trend observed was the declining use of Remote Desktop Protocol (RDP) practices to gain initial access to target systems. This may be because potential target organisations are protecting themselves better from attacks of this kind or because a large proportion of the vulnerable configurations have already been exploited. As RDP services decline as an initial access route, other ways in such as phishing and access through third parties is increasing as a proportion of all attacks.

NCSC VIEW: FUTURE THREAT CHALLENGES

Proliferation of cyber capabilities

In the coming years, the NCSC anticipates that the proliferation and commercial availability of cyber capabilities will expand the cyber security threat to the UK. In the future, 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 with less predictability.

This wide and complicated landscape includes the provision of off-the-shelf cyber surveillance products and supporting services, the vulnerability and exploit marketplace, hackers-for-hire offering bespoke hacking services and the use of commercially or publicly available malware.

The growing grey market for cyber tools lowers the barrier to entry to states in obtaining capability – some of which will be highly advanced and sophisticated – and therefore the intelligence that they would not otherwise develop or acquire. Demand for these products and services is such that we expect the sector to continue to grow.

Hackers-for-hire and 'As-a-Service' models are also lowering the barrier to entry for non-state actors. Ransomware as a Service (RaaS) is an example of how this proliferation is allowing less sophisticated criminal actors to extort organisations. We are also seeing emerging use of hacking services in corporate espionage.

In June 2022, Lindy Cameron highlighted the challenge that proliferation of cyber capabilities presents in a speech during Tel Aviv Cyber Week, stating: "If we are going to maintain a cyberspace which is a safe and prosperous place for everyone, it is vital that such capabilities are produced and used in a way that is legal, responsible and proportionate.[15]

[15] https://www.ncsc.gov.uk/news/lindy-cameron-at-tel-aviv-cyber-week

In addition, the geopolitical landscape has also spurred on the actions of non-state actors; cyber criminals, and 'hacktivists' with economic or political motivations. We saw this following the Russian invasion of Ukraine and while we cannot predict the long-term impact of these actors, the impact of their actions will continue to shape the cyber landscape.

Supply chain attacks:

The technology ecosystem that we all rely on is continuing to grow rapidly – and becoming increasingly complex. This size and complexity create increased opportunities for criminals and states to achieve their ambitions.

Supply chain attacks are an example of how this increasingly complex technology ecosystem can be exploited. Where organisations cannot directly be compromised, an adversary can take advantage of lax security somewhere in that organisation's digital supply chain.

This came to prominence with the 2020 compromise of SolarWinds by the SVR However, the threat to technology supply chains is much broader than this isolated case.

Over the last year, the threat to global IT infrastructure from foreign states and cyber criminals has almost certainly grown as both continued to develop their capabilities against the IT sector. While foreign states target entities for intelligence gain, cyber criminals targeted them largely to carry out ransomware or data extortion attacks for profit.

Paul Chichester, Director of Operations NCSC

CHAPTER 2 – RESILIENCE

Introduction

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 the 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 getting through. In total, 2.1 million malicious cyber campaigns were removed this year. At the same time the NCSC engaged and equipped citizens and sectors with new and updated resilience advice, tools and services. And in partnership with the government, industry, law enforcement and other agencies it 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 as a core part of organisational risk management through use of regulation and other incentives;
- harness the power of threat insight to build communities that can defend themselves.

This chapter sets out more detail about how the NCSC helped to bolster the UK's cyber resilience and describes some of the key issues and actions that need to be considered to fulfil the ambitions in the NCS.

Ransomware

The resilience story this year can be told through the "three Rs": ransomware, Russia and renewal. While one of the most high-profile and concerning cyber risks came from Russian cyber aggression related to their invasion of Ukraine, it was another "R" that required much of the NCSC's focus on resilience this year: ransomware.

With ransomware continuing to be a significant threat, the NCSC joined government, NCA, Regional Organised Crime Units, police forces and the cyber security sector to improve resilience by stopping attacks getting through, calling out threat actors, reviewing policies, fine-tuning practices and working internationally to tackle this global issue. The NCSC took a three-pronged approach:

- Alerting audiences to the latest threats, risks and vulnerabilities and updating and clarifying advice and guidance in how to respond 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.

A government ransomware "sprint", led by the Home Office, improved understanding of the scale and complexity of the threat, and helped it to better prioritise, focus resources, refine advice and be more targeted in its engagement.

As part of the NCSC's contribution to the UK's international co-operation on this threat, in September, senior UK and US cyber security leaders met to discuss shared threats and opportunities and reaffirm their commitment to tackling ransomware. In February the NCSC joined US and Australia to reveal growing sophistication of ransomware and urged businesses to take protective action against increasingly professional criminal attacks.

To support organisations improve their own resilience, in March, the NCSC launched a new ransomware portal with refreshed advice and guidance, including practical resources to help users prevent, report, respond to and recover from attacks.

NCSC's key actions to prepare for ransomware:

- make regular backups
- prevent malware from being delivered and spreading to devices
- prevent malware from running on devices
- prepare for an incident

More advice can be found on the ransomware portal

Russia

Weeks before Russia's invasion of Ukraine the NCSC updated its guidance and alerted UK Government, businesses, organisations and citizens about the actions to take in the event of a heightened cyber threat. This included fundamental protections such as patching, backups, incident planning and systems monitoring.

As the attack grew closer 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 were shown to have been critical in protecting the Ukrainians against Russian cyber attacks, and raising the country's general cyber resilience.

Closer to home, Sir Jeremy Fleming and Lindy Cameron led roundtables with CEOs of domestic energy, utilities, food, communications, transport and other essential service providers to brief them on the risks and mitigations to help minimise impact should Russian cyber aggression reach or impact the UK.

As the conflict took hold, the NCSC increased its engagement across sectors and institutions. This included several Digital Loft briefings which reached thousands of businesses and organisations.

As well as direct engagement, further public announcements and advice on strengthening defences were made throughout the early stages of the invasion, with the NCSC highlighting the potential for burnout among cyber defenders and setting out steps that organisations could take to reduce this risk.

This activity was complemented by four audience-led communication campaigns running in the first two months of the conflict which saw NCSC advice and guidance reaching millions of citizens and small businesses through radio, social media and partnership channels, leading to significant increases in downloads of cyber resilience resources from the NCSC website.

During this period there was a 41% increase in unique visits to ncsc.gov.uk, peaking on 24 February, which saw visits 147% above the average daily rate. Visits to critical guidance such as the Small Business Guide, and advisories such as 'Actions to take when the cyber threat is heightened', saw increases of up to 900%.

Resilience renewed

While ransomware and Russia attracted a particular focus this year, the NCSC ensured a "threat-informed" approach in its continued resilience-building across a wide range of sectors in the face of a sustained threat and risk to businesses and organisations.

Earlier this year it was revealed that 39% of businesses in the UK had suffered a cyber attack over the previous 12 months, 20% of which faced a material outcome, such as loss of money or data.

As well as threats and risks, the NCSC continued to observe the impact and potential harm from critical vulnerabilities in the global IT system. One of the most serious this year was linked to the Log4j logging system that was present in millions of computers around the world.

The vulnerability, if left unfixed, meant that attackers could break into systems, steal passwords and logins, extract data, and infect networks with malicious software. As countries and institutions raced to patch the vulnerability, the NCSC took a leading role in alerting UK organisations and businesses, and providing them with advice and services, such as Early Warning, which notifies users about potential threats, risks and vulnerabilities on their systems.

The NCSC's general 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 advice, guidance, tools and services, giving them agency to apply these resources to help improve their resilience.

Reducing the burden

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

This included providing insight, evidence and technical advice to the government for the development of the Product Security and Telecommunications Infrastructure Bill, which will require manufacturers to ensure minimum security requirements are met in relation to consumer connectable "smart" products.

In May a new data sharing capability, which helps block access to scam websites instantly was announced. The new tool was made available to all UK internet service providers (ISPs) allowing them to block websites flagged as fraudulent. The "landmark partnership" with ISPs means that scams can be blocked from ever reaching the average citizen online.

Active Cyber Defence

One of the most important initiatives pioneered by the NCSC is its Active Cyber Defence (ACD) programme. The core premise of ACD is to tackle high-volume commodity attacks that affect people's everyday lives, doing small things at scale that add up to make a big difference.

In May, the NCSC published its fifth report into ACD, setting out the programme's impact so far. Notably this year, the Suspicious Email Reporting Service reached 10 million reports, resulting in the take-down of 76,000 scams. By the end of August 2022, the number of reports (since April 2020) had risen to 13.7m, while the number of scam URL addresses taken down, that were previously unknown to UK authorities, had risen to 174,000.

In April the NCSC opened its Web Check and Mail Check services to the whole education sector for the first time to protect websites and email servers of schools, colleges and universities from cyber attacks.

One of the newest ACD services, Early Warning, which is free and open to any organisation, had, by the end of August 2022 sent 34 million notifications to its 7,500 and growing members to inform them of threats, risks, vulnerabilities and open ports in their networks.

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.

ACD services and results

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

- Organisations using PDNS rose **23%** (from 928 to **1140**)

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

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

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

- Over 750 reported vulnerabilities across the UK government remediated

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 1386 to **2448**)
- **Domain Messaged Authentication Reporting** (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 3000 charities

Email Security Check is 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

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 take downs 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 54% (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 3539 to 4849)
- 43% increase in unique URLs scanned using Web Check
- 12.5 % increase in urgent findings reported to users, along with remediation advice

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 3924 to 7523)
- 34 million notifications issued about potential threats, risks, vulnerabilities or open ports in user's networks

Coming next for ACD

In the coming year the NCSC is expected to increase the scale and scope of ACD further. This includes releasing its first service designed for small businesses and organisations, who run their own website, email domain or office file server, to improve understanding of their potential vulnerabilities. While this is designed to be a practical and easy-to-use tool – and free to any UK organisation – the NCSC is confident it has the potential to require cyber criminals to "raise the bar" to carry out successful attacks.

Behind the scenes the NCSC is also working to improve ACD services for security professionals in larger organisations, particularly those in the public sector and operators of critical national infrastructure. They are expected to see services, such as vulnerability scanning, being expanded, deepened and coming together in a more consistent way.

Resilience tools and services

The NCSC's website continued to be its online centre for its latest advice, guidance, blogs, tools and services. A total of 18 new pieces of guidance were published in 2022, along with 50 blogs on a range of topics, with over 1.6 million unique user visits. The most searched terms were "password(s)" and "phishing", with 4,051 and 3,518 unique searches respectively.

While there is a large range of resources on the NCSC's website, the following are some of the key products for general cyber resilience, many of which were refreshed this year.

Audience	Resources and tools
Citizens and families	Cyber Aware
Sole traders & microbusinesses	Cyber Aware Action Plan Small Organisations Newsletter

Small & medium-sized enterprises	Small Business Guide: Cyber Security Small Organisations Newsletter Training for small organisations	Exercise in a Box NCSC's A-Z of cyber security Supply Chain Guidance SOC Guidance Early Warning Active Cyber Defence
Medium & large organisations	Device & risk management Board Toolkit Cyber Assessment Framework 10 Steps to Cyber Security	

Resilience round-up

Equipped with up-to-date insights on threats, risks and vulnerabilities – and with new and refreshed tool and services – the NCSC sought to engage, influence and shape the whole of society's efforts to bolster the UK's resilience, as thus:

- Guidance for retailers to prevent websites becoming Black Friday cyber traps was published in November. The NCSC notified over 4,000 small business sites whose customers' payment details were being stolen after it identified that hackers were exploiting a vulnerability in popular e-commerce software. Later that month the NCSC alerted Christmas shoppers about keeping secure online over the festive period.
- Launched its new-look Cyber Essentials scheme to support organisations to stay ahead of the cyber threat. This followed a major review of the scheme, which remains a key tool to help any sized organisation improve their resilience through the implementation of five key technical controls and protects them against most common, internet-based attacks.
- New guidance for organisations who used SMS and phone calls to communicate with customers and service users was published in January. The telephony best practice was produced to help businesses reassure their audiences by ensuring messages were consistent, trustworthy, and reached customers without being blocked or deleted as suspicious. This came at a time when cyber criminals continued – albeit in smaller numbers – to spoof identities of trusted and well-known organisations, such as the NHS or HMRC.
- Launch of latest Cyber Aware campaign in March urging citizens, sole traders and microbusinesses to improve their email security by adopting two-step verification and a strong and separate password using three random words.
- Recognising that the supply chain for IT and technology services is a common vector for cyber attacks, the NCSC alongside international partners published updated related guidance.
- In April the latest version of the NCSC's Cyber Assessment Framework (CAF) was published. The CAF was first launched in 2018 to assess how well suppliers of essential services were managing cyber security risks. Version 3.1 was released to support core users, including CNI organisations and those subject to Network and Information Systems (NIS) Regulations.

- Welcomed the publication of the first ever Government Cyber Security Strategy (GCSS), setting the approach for cyber resilience to 2030.
- Related to the GCSS, in a blog published later in the year, the NCSC explained how CNI organisations could improve the security posture of their internet-facing services.
- At the NCSC's annual flagship event, CYBERUK in May, it launched its new email security tool to help organisations check their defences. The free service was developed to help organisations to identify vulnerabilities that could lead to spoofing or email privacy being breached.
- In July the NCSC announced the new Cyber Advisor Pilot Scheme: a new initiative that offers assured cyber security consultancy services to small and medium sized companies, helping them achieve a minimum standard of security.
- Schools continued to use the NCSC's training for teachers and school staff. By July, views of the video resource on YouTube had exceeded 138,000.
- In August construction firms working on major building projects, such as HS2, were offered bespoke advice aimed at helping them keep sensitive data safe from attackers: an important step in maintaining the integrity of projects critical to the UK's future infrastructure.
- Throughout the year, the NCSC continued to provide advice and support to Parliamentarians and senior government officials in the use of their work and personal systems and devices to prevent hostile actors accessing classified or sensitive information.
- As well as supporting cyber security aims, the NCSC sought sustainable outcomes to extend the life of devices, including longer manufacturer support periods for devices and advice for those repurposing second hand devices.
- Whilst necessarily not in the public eye, the NCSC continued to work on one of its most important duties: supporting the UK's Armed Forces, from protecting the integrity of their digital-dependent assets from cyber threats to the development of future cyber defence capability.

Critical National Infrastructure and essential services

Over the past five years the government has focused heavily on improving CNI cyber security, and the NCSC has been central to the collective efforts to "raise the bar" for resilience across the whole sector.

This included mapping UK CNI systems (including their interdependencies and supply chains) to ensure a wider understanding of what is critical and why. This year such mapping, which is enabled by the NCSC, allowed the government to identify previously unknown CNI systems and therefore improving its understanding of the landscape.

The NCSC continued to drive information-sharing groups across CNI sectors, including the Financial sector cyber collaboration centre (FSCCC), which supports industry to build and develop closer information-sharing and collaborative groups. Within the most critical sectors where there are the most significant risks, the NCSC continued to provide direct industry

support with a greater focus on providing solutions at scale, such as Active Cyber Defence (ACD) services.

NCSC view: actions for a resilient UK

This year the NCSC continued to work tirelessly to bolster the cyber resilience of the UK, which has, in our view, contributed to cyber attacks being prevented and harm being reduced.

As we have often said, cyber security is a team game. We are proud to be the captain of that team and I am pleased to see that significant steps have been taken to increase resilience across so many sectors. Events like the Russian invasion of Ukraine, Log4j and continued ransomware attacks highlighted the need to bolster cyber resilience.

However, as the UK's technical authority it is our duty to highlight – and help close – serious gaps in the nation's cyber defences. While 2.1 million attacks were stopped over the past 12 months too many still get through. Breaches affect government, businesses, organisations and individuals. Poor organisational practices, processes and systems, and lack of awareness of risks and mitigations, all contribute to attacks getting through. Taking some practical and cost-effective steps, such as improving the use of account authentication, could have prevented a lot of damage.

Earlier this year it was revealed that 39% of businesses had identified a cyber attack. Many of these businesses suffered a material outcome, such as loss of money or data. So, for the UK to meet the ambitions set out in the National Cyber Strategy there needs to be a holistic, whole-of-society effort to improve resilience across the country.

It is right for government to focus on steps to secure the digital environment for all UK internet users, to prevent attacks, build basic security in products and services, and help individuals and small businesses and organisations with practical actions to improve cyber security.

This must be a shared endeavour between the government and all parts of the economy and society. It is the responsibility of boards of businesses and organisations to manage their own cyber risk – informed, in part, by the NCSC's assessments and insight.

Meanwhile, government departments, the wider public sector and regulated operators of CNI, must raise their standards and manage their risk more proactively. Large businesses and organisations, including providers of digital services and platforms need to be more accountable for protecting their systems, services and customers as a core part of running their business.

In return, the government must continue to help secure the digital environment and tackle systemic risks and provide support through advice, tools, accreditation in the marketplace, and developing the skills that enable improvement.

For the NCSC this means continuing to help organisations to understand the threats, risks and vulnerabilities and working in partnership to implement the behaviours, responses and actions that will help fulfil the vision of making the UK the safest place to live and work online.

Paul Maddinson, Chief Operating Officer NCSC

CHAPTER 3 – TECHNOLOGY

Introduction

This year the NCSC continued to develop insights, capabilities and principles to help ensure critical technology was secure, resilient and reliable to protect data, devices and services that underpin the UK's national, economic and security interests, 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 become more embedded in the daily lives of citizens, businesses and essential services. Technology continued, in part, to be the subject of geopolitical competition between states who see, and begin to realise, the opportunities of technology advantage.

As this competition grows and becomes more diffuse, the UK faces an increasingly fragmented technology ecosystem which creates risks for interoperability and the values that underpin it.

This chapter sets out how the NCSC continued to innovate and build capability to help keep up and ahead of the ever-evolving threats, risks and vulnerabilities, while providing insight, evidence and expertise to help the UK adopt a values-driven approach to the development of future technologies.

National context

When the government established the NCSC in 2016 their focus was primarily domestic and aimed at ensuring proactive state intervention to reduce threats to UK systems, organisations and citizens.

The new National Cyber Strategy broadened the emphasis to include offensive, as well as defensive, capabilities and objectives, and shifted from a largely domestic focus to one that recognises that today's challenges are increasingly international.

This new focus was in recognition of technology leadership shifting to authoritarian regimes in South-East Asia in a trend that could have profound implications for Western-style democracies. China's strategy of protecting its domestic market while exploiting global trade has existed since the 1990s. However, in the last five years China has extended its effort from dominating technology manufacturing to influencing the foundational rules that define the next generation of technology design and development.

Over the past year, the NCSC continued to track and assess the implications and risks of key areas of this shift in leadership: technology standards and digital dependence, and the implications of both.

Technology standards

The current internet relies on protocols designed by its founders in the 1960s and 1970s. It reflects the vision of technologists who did not want centralised control, and who set out to design an architecture that was open, resilient and neutral. It is clear that China is seeking to supplant the originating, founding principles that underpin today's technologies and implant their authoritarian traits of surveillance and control into tomorrow's. This can be seen through its "standards strategy", including filling key positions on Standards Development Organisations (SDOs) and other international forums, and their proposals of a "top down" and "centralised control" approach for the design of the future internet.

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 one ecosystem dominated by the "West" and one that is dominated by China.

Digital dependence can also be seen in other ways. As China extends the use and influence of its technology, via the *Digital Silk Road* initiative, third-party countries dependent on Beijing's support for their digital infrastructure are arguably more likely to support them in international institutions, such as the UN or WTO. The technology itself creates a dependency as once it is installed it is expensive to remove. Even those countries who disagree with the values that are attached to Chinese dependency may choose to accept them for their own national interests.

Fragmentation

The combined effect of changes in standards and the split into multiple ecosystems has led commentators to talk of the acceleration of harmful forms of fragmentation of the internet. While the internet, due to its decentralised evolution, has always been fragmented to a certain extent, what linked it together were fundamental 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 could not use their mobile phones in the United States. 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 their privacy, security or functionality.

The NCSC believes this has significant implications for the UK's cyber security. As seen in the National Cyber Strategy there is an emphasis on projecting UK leadership in the technologies that will help the country cement its position as a leading, democratic cyber power. This includes leadership in shaping the UK's future telecoms systems and limiting reliance on suppliers or technologies that are developed under regimes that do not share the values of free, open and democratic societies.

The NCSC's response

To address this, the NCSC stresses the importance of:

- Increasing co-operation and co-ordination between allies to promote and instill their shared values into the design and development of technologies societies depend on.
- Supporting a multi-stakeholder approach to standards development, and 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 invest in foundational science, research and development, and early-stage industrialisation30, and ensuring this research is protected from hostile activity.

As well as providing technological insight to support a values-driven approach to the development of tomorrow's technologies, the NCSC continued to innovate and build capability for others to benefit from today.

The NCSC's **National Crypt-Key Centre** (NCKC) continued to be the central focus for how the UK develops, operates and maintains the systems providing highly secure communications for the government, military, industry and national security partners. In May, the NCSC welcomed the National Security Council's decision to approve the National Crypt-Key strategy; for the first time setting out a cross-government approach to the development, management and support to the UK's use of cryptography to protect its most critical information and services.

In August, the NCSC issued its **Principles for the Security of Machine Learning.** Due to the increasing presence of these systems in many aspects of life, from providing the 'smart' in smartphones to critical areas like healthcare, finance and national security, the NCSC sought to inform and equip users to help secure their personal or organisational systems, information and data.

Other key developments in technology capability included:

- The NCSC worked to support mobile network owners in the UK to improve the security of their services. The NCSC developed and delivered a new tool, filling a critical gap, that will **help discover new mobile network vulnerabilities.** In addition, in partnership with Mobile Network Operators, the **NCSC developed a National Telecoms Signal Monitoring Service** (NTSMS) to understand the threats to our networks, to inform and improve defences and to support incident investigation.
- The NCSC **supported the introduction of new UK legislation.** The Telecommunications (Security) Act which received Royal Assent in November 2021 will improve the security of our digital infrastructure. The Act introduces a stronger telecoms security framework which places new security duties on public telecoms providers, and new national security powers to address the risks posed by high-risk vendors.
- The NCSC also assisted with the development of the new Electronic Communications (Security Measures) Regulations drawn up under the Act.
- The **Product Security Act** was laid before parliament. This will provide Government with the powers to set security requirements for consumer devices, and to enforce when

those requirements are not met. The NCSC **launched the Device Security Principles** for Manufacturers (Beta). The Device Security Principles is a guidance collection designed to help organisations gain confidence that Enterprise Connected Devices are protected against common cyber security threats and risks.

- Refined guidance to help citizens and organisations, from advice around 'Bring Your Own Device' approaches in business networks to best practice for backing up data. Much of this contributed to the updates to **Cyber Aware** (for the citizen) and **Cyber Essentials (for businesses)** throughout the year.
- Published research papers and blogs throughout the year, including on zero trust for customers looking to begin a migration journey to a zero trust architecture.
- Updated all **cloud** guidance to reflect how much cloud services have changed in the past decade.
- **Supported HMG's development of its Artificial Intelligence strategy** in collaboration with DCMS, and continued to invest in understanding of the threats and ethics around AI. Later in the year, the Alan Turing Institute won an international competition for their NCSC-sponsored work on AI in autonomous cyber defence.
- Notified Google about 15 **suspicious mobile applications** that were either advertised as SIM farms or offered customers incentives to persuade them to use their tariff contrary to their Terms and Conditions. This notification resulted in Google removing most of the offending apps.
- Published its **guide to Vulnerability Discovery and Disclosure** helping companies of all sizes implement robust vulnerability disclosure processes. The guide was also published by the International Standard Body, ETSI.
- Held two conferences **(Safety, Security and Verification in Critical Systems** and **VICECon)** bringing experts together to share on topics around vulnerability research and sharing.

NCSC view: future technology challenges

As digital technology integrates into our lives, our businesses and our infrastructure, some technologies are becoming central to the way we live. Countries that have a strategic advantage in science and technology and can drive innovation will be well placed to exert influence over others and shape global standards in ways that suit their own economic and political interests.

In response to the changing nature of the challenges to our cyber security the 2022 Cyber Strategy had two central aims. The first was to take the lead in the technologies that are critical to the future of cyber power, such as Quantum Technologies, Artificial Intelligence, Semiconductors and Future Telecoms. The second was to limit our reliance

on individual suppliers or technologies that are developed under regimes that do not share our values, and to diversify markets.

We face an unprecedented set of issues and resolving them will require similarly unprecedented levels of innovation and co-operation between allies. To strengthen the Western influence in SDOs, we need to bring together our effort, focusing on critical technologies and taking action that both protects the global market and safeguards the SDOs themselves. Our best interests are not likely to be served by accepting further bifurcation of technology groupings, into one driven by the West and one by China. China has shown that it is prepared to invest to build market penetration around the world and its internal market is big enough to support a sovereign stack, and so we must be smarter in how we now respond.

A few technologies will have such far-reaching implications both for society and for national security that we must act in ways that are not solely driven by commercial considerations. As an example, quantum computing has the potential to radically change our society, and to damage our security if it is in the hands of our adversaries at an early stage. The UK is home to some of the most cutting-edge quantum computing research globally and it is essential that the underpinning science, engineering and industrialisation are protected from adversaries. Measures such as the National Security and Investment Act are important, enabling us to protect our market where predatory interventions impact our national security, but more thinking is needed on ways to help these ecosystems thrive while mitigating the risk of relying on an unconstrained global market or limiting open science.

We must remain committed to supporting the underpinning science, research and development, and the building of new products and industries. We must also make our supply chains resilient to shocks and able to mitigate interference from our adversaries. However, the real opportunity for our strategic advantage is for the markets to be shaped to opt for our technologies and products reflecting our values, rather than those of our rivals. As technology becomes an increasingly important aspect of geopolitical power, we must expect competition in this arena to further intensify.

Dr Ian Levy OBE, Chief Technical Officer NCSC

CHAPTER 4 – ECOSYSTEM

Introduction

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.

This aim was reinforced as one of the five pillars of the government's National Cyber Strategy, with investing in cyber skills being a vital part of that goal.

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

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

In February, analysis revealed record levels of growth were apparent 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.

However, it is evident the sector faces challenges when it comes to optimising growth, skills and diversity. Over half of businesses lack basic technical cyber skills and there is an annual shortfall of over 14,000 people in the UK cyber security workforce.

Too many vacancies go unfilled, the pipeline of talent falls short of the numbers it needs, while its workforce does not always reflect the diversity in wider society. The second joint **NCSC-KPMG Decrypting Diversity report,** 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. In her foreword, Lindy Cameron described the report as a "wake-up call" and called on industry to come together and act on its recommendations.

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, through its people, projects and initiatives is looking to fill gaps and create a world-class cyber ecosystem.

Engaging young people

The NCSC's **CyberFirst** programme, which provides opportunities for young people to get into cyber security, continued to grow this year. The popular initiative covers a broad range of activities: a comprehensive bursary scheme to financially support undergraduates through university and a degree apprenticeship scheme; a girls' competition; thousands of free places on CyberFirst courses at UK universities and colleges; and the CyberFirst Schools and Colleges project.

More than 7,000 girls took part in this year's Girls Competition. 130 teams comprising 12- & 13-year-olds from across the UK reached 13 regional and national finals in February where they overcame challenges in range of topics, including networking, artificial intelligence, cryptography and logic.

The in-person finals – after having gone online during the Covid pandemic - were supported by organisations from industry and academia, whose partnerships with the NCSC are becoming increasingly important in strengthening the UK's thriving cyber security ecosystem and developing the next generation of cyber security experts. 50,000 girls have now taken part in the competition since 2017.

Some of those early finalists are now working in GCHQ or receiving financial support through the CyberFirst Bursary scheme while studying at university.

While CyberFirst is open to all young people, the emphasis on a girl's competition is aimed at bolstering female representation in the cyber security sector, which accounts for just 16% of the workforce.

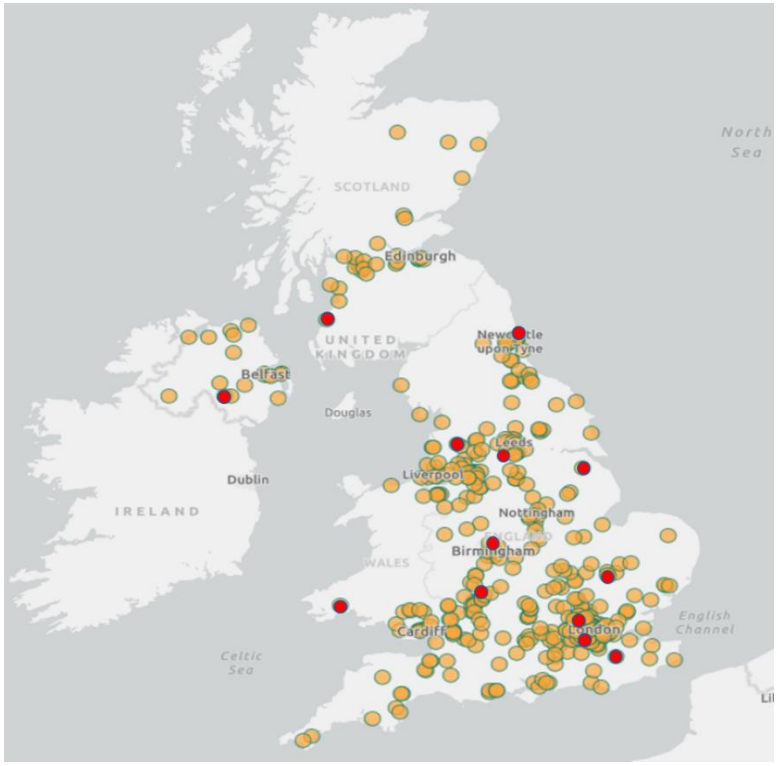

Image: Map of schools participating in CyberFirst Girls Competition. Winning teams are marked by a red dot.

The **CyberFirst Schools & Colleges** scheme, which recognises academic centres for excellence in cyber security education, saw eight more establishments join the fold this year. The schools and colleges received CyberFirst status for delivering first-rate technology and cyber security teaching in and out of the classroom.

Since the initiative launched in 2020, 57 CyberFirst Schools and Colleges have been recognised for their excellence in developing cyber skills ecosystems around the country and addressing the industry's cyber skills gap.

Like other holders of this status, the new schools will benefit from opportunities to engage with local and national businesses and universities who have offered their time, expertise and resources. They can also be expected to be a focal point for other CyberFirst activities and provided with an opportunity to be a part of CISSE UK.

In February, a new CyberFirst-related learning platform was launched by DCMS to help teach 11-14 year olds essential digital skills to improve their online security as well as encouraging careers in the sector. The Cyber Explorers teaching resources – part of the CyberFirst family of schemes - were brought together in an interactive cyber security learning platform being rolled out across UK secondary schools this year.

After being launched in 2021 the NCSC's CyberSprinters video game for 7-11 year olds was updated this year with new stories and features. The game, which introduces players to cyber security, is supported by a suite of resources for teachers but can be played without supervision.

Further and higher education

The **CyberFirst Bursary** programme continues to support the next generation of cyber talent, with a £4000 bursary to undergraduates and paid cyber security training each summer. This year, a further 85 students joined the bursary scheme with a 42% female intake and 23% from ethnic minority backgrounds.

In total, over 1000 students have benefited from these bursaries, 93% of whom are now in cyber security roles in an industry where the average salary is an estimated £60,000 per year. The bursary scheme and wider ecosystem is now supported by over 200 members organisations from industry, academia and government.

For Higher Education the number of NCSC-certified **Academic Centres of Excellence in Cyber Security Education** grew to 13. Since its launch in 2020, the ACE-CSE programme, led by the NCSC and DCMS has recognised UK universities with gold and silver awards for showing their commitment to delivering first-rate cyber security education on campus and beyond.

This year saw Cardiff University added to the list of recognised institutions across England, Wales, Scotland and Northern Ireland. ACE-CSE universities continued to play a key role in bringing together stakeholders to develop, shape and support cyber security education to meet the needs of the local population and employers.

The ACE-CSE programme builds on the NCSC's existing degree certification programme, which helps set high standards of cyber security teaching across higher education as well as helping students make informed decisions about the range of courses on offer at UK universities.

This year, 18 postgraduate and three undergraduate **degree courses** in England & Wales were NCSC-certified, as well as two Scottish Graduate Apprenticeships. More than a third of UK universities now offer postgraduate degrees in cyber security, certified by the NCSC. Overall, a total of 63 degrees from 41 universities throughout the UK have been certified.

Offering an NCSC-certified course benefits institutions by raising their profile and improving the quality and number of applicants. Official data showed that more than half of UK students (52%) pursuing a cyber security-related Master's degree chose an NCSC-certified course.

Innovation and growth

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 to work in teams to find innovative solutions to two cyber security challenges facing the UK: securing the supply chain and safe remote working.

The **NCSC for Startups** initiative continued to translate talent into jobs, opportunities and growth this year. The project, which is delivered between the NCSC and Plexal, in partnership with Deloitte, CyNam, Hub8 and QA, nurtured and advised fledgling cyber security businesses by enabling them to develop, adapt or pilot technology to meet big challenges in the sector.

Over the last year, 14 new organisations were onboarded to the initiative, taking the total number of participants to 62 since the scheme started in 2017. Employee headcounts at businesses which have gone through the scheme increased from 475 to 1210, and investment to date went from £100 million to more than £422 million.

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.

Lawyers, analysists and chief technology officers for multinational cyber security companies were among some of the i100 participants who joined NCSC teams on a part-time basis. Like other participants they got an opportunity to work on a range of strategic and tactical activities.

Setting, certifying, assuring and testing standards, products and services

A key feature of the NCSC's ecosystem development work is its **standards-setting, and industry assurance, certification and testing schemes.** This year the NCSC relaunched schemes such as Cyber Incident Response, while introducing new initiatives and standards to harness more talent in the ecosystem, broaden the market and allow a wider cross section of industry to work with the NCSC or find support from the 400+ organisations assured by it.

The NCSC broadened 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 a new application process for the Cyber Incident Response scheme.

The scheme supports 'high threat' organisations of national significance and was relaunched at the end of March as Cyber Incident Response Level 1. Work has continued on a new Level 2 scheme, which is expected to support the growth in the sector while extending the reach of the NCSC in providing incident-response support to medium and large enterprises, local authorities and other government bodies.

This year, a new Cyber Incident Exercising pilot was successfully completed, with the findings enabling the NCSC to deliver a controlled, scenario-based platform for organisations who want to practice, evaluate and improve their cyber incident response plans in a safe

environment. An Expression of Interest was released earlier this year to find a partner to help deliver these new schemes.

Since the formation of the UK Cyber Security Council (UKCSC), the self-regulatory body for the cyber security profession, the NCSC has worked closely with them on a range of shared challenges. In May it was announced that the NCSC was working to pass the stewardship of the Certified Cyber Professional (CCP) scheme to the UKCSC.

In July, the NCSC launched a new Cyber Advisor scheme with 100 fully funded assessments of potential Cyber Advisors to confirm they possessed a good understanding of baseline security controls and the ability to provide practical help to companies who wanted to achieve them.

The scheme is planned to go live next year and will offer assured cyber security consultancy services to a wider market of small and medium sized firms, helping them to meet minimum standards of security.

Cyber Advisor organisations will be able to provide customers with practical help to achieve a basic level of resilience. Advice will initially be focused on Cyber Essentials' five technical controls – firewalls, secure settings, access controls, malware and software updates – and qualified Cyber Advisors will help customers meet these controls and implement any recommendations.

As well as launching Cyber Advisor, the NCSC refreshed the Assured Cyber Security Consultancy scheme, and developed a new standard, assessment criteria and assessment process. These updates have been implemented by the NCSC alongside input from scheme members. The scheme continued to deliver tailored cyber security consultations on complex issues to government, public sector organisations and the UK's CNI.

NCSC view: future ecosystem challenges

A robust, self-sustaining cyber ecosystem is mission-critical for the UK's national security interests and has a stake in making the country a global leader in critical technologies. It is also a dynamic part of the UK economy with a £10 billion contribution to the UK's economic growth agenda.

This is why the NCSC continues to do work with the Department for Digital, Culture, Media and Sport to create a cyber ecosystem that can safeguard the digital landscape, nurture skills and translate them into commercial success stories.

Achieving this aim will take ambition, investment, dedication and collaboration between government, academia and industry. These partnerships can become greater than the sum of their individual parts and create the perfect environment for a dynamic and trusted ecosystem to flourish.

Whether it is finding, nurturing and developing a diverse and technically skilled workforce of the future or harnessing the innovative talents of the UK's vibrant research community, the NCSC has focused on fortifying the UK cyber ecosystem through a series of projects and initiative, especially at the local level.

As well as nurturing talented young people into the cyber security sector via CyberFirst initiatives, the NCSC for Startups initiative continued to translate talent into jobs, opportunities and growth. So far, the alumni have raised over £422m in funding and created over 700 new roles.

A key focus of the ecosystem development work is the NCSC assurance schemes for industry. These harness the talent in the ecosystem to increase the impact of the NCSC. This year as well as relaunching schemes like Assured Consultancy and Cyber Incident Response, new schemes are being developed that will broaden the market and allow a wider cross section of industry to work with the NCSC or find support from the organisations assured by them.

While considerable progress has been made in strengthening the UK's vibrant ecosystem there are still big challenges facing it. The 14,000 annual shortfall of staff in the sector will hold it back, as will the shortage of skills and diversity within it.

Much has been studied and written about the cyber security industry, where extensive data and research has provided key insights, evidence and lessons. This includes publications about workforce, labour market, skills and equality, diversity & inclusion. These have helped describe the issues but more importantly they have set recommendations to help address them.

I have now worked in cyber security for many years, well before the phrase was coined. What I have learned during that time is that building national capabilities takes a national effort, but delivery is most successful when it brings together the talents at a local level. Whilst we continue to deliver that national agenda through things like our support for the UK Cyber Security Council, our focus is shifting towards a more local approach. This is why we call on our many existing academic and industry partners to consider what more they can do to support these activities in their local areas.

Chris Ensor, Deputy Director Cyber Skills and Growth NCSC