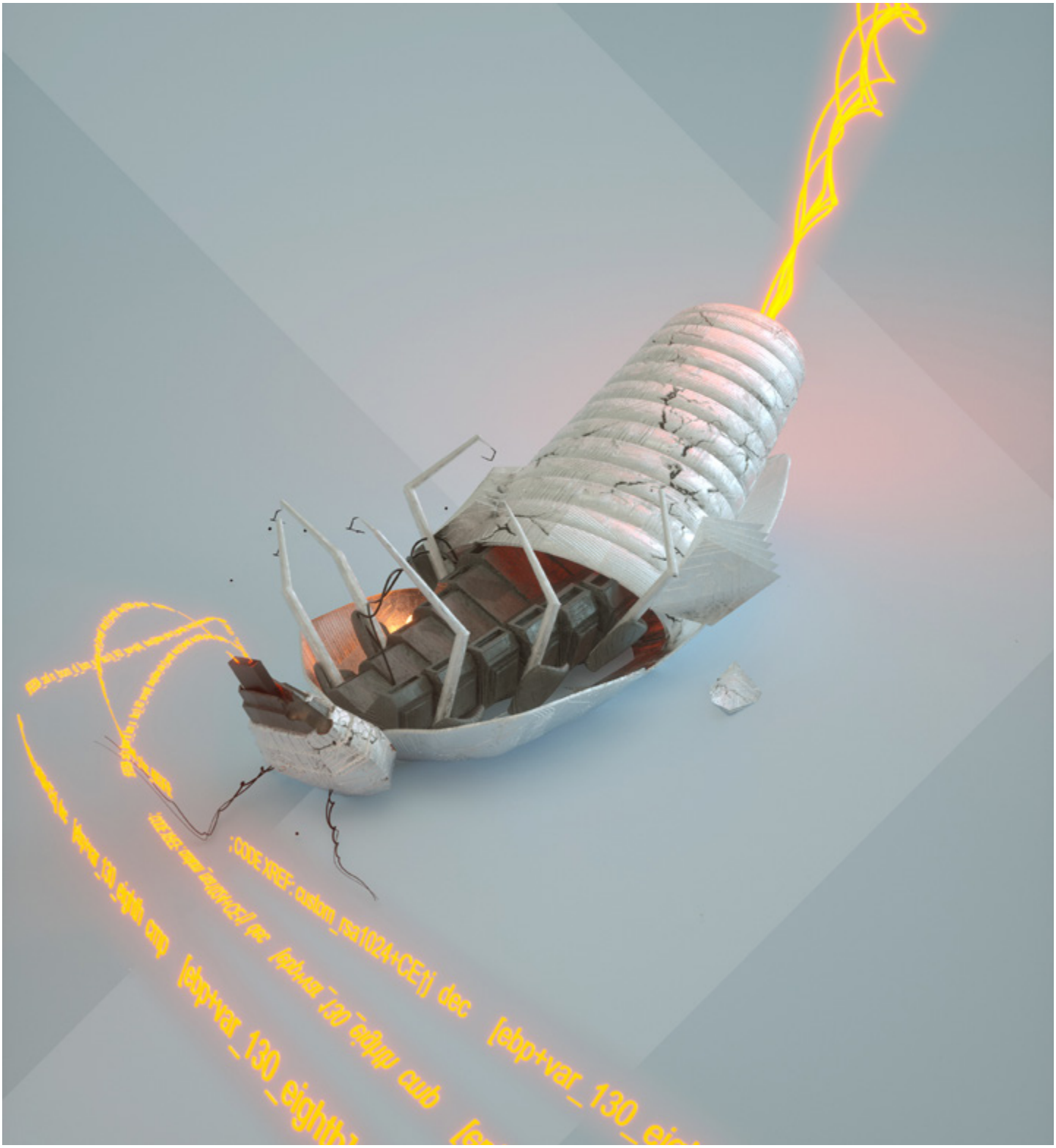
National Cyber Security Centre
a part of GCHQ

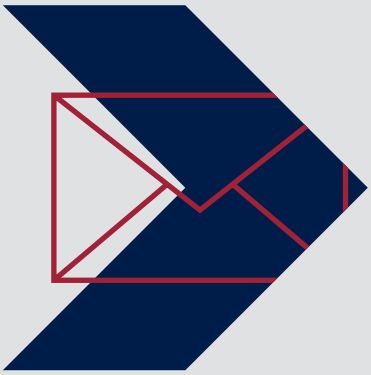
Annual Review 2021

Making the UK the safest place to live and work online



How to report suspicious emails, websites and text messages

- If you have received an email which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS) at **report@phishing.gov.uk**

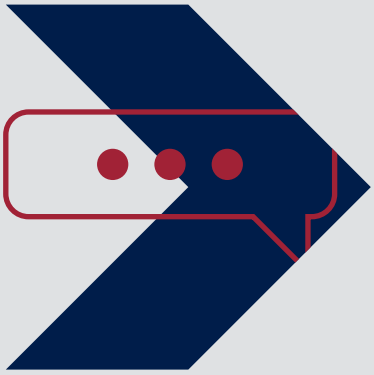


- If you have come across a website which you think may be fake and is trying to scam you, visit **ncsc.gov.uk/section/about-this-website/report-scam-website** and follow the instructions

- Phone providers allow you to report suspicious text messages for free using the shortcode **7726**.

  If you forward a text, your provider can investigate the origin of the text and take action, if found to be malicious.

  If 7726 doesn't work, you can find out how to report a text message by contacting your provider.



The National Cyber Security Centre (NCSC), a part of GCHQ, is the UK's technical authority for cyber security. Since the NCSC was created in 2016 as part of the Government's National Cyber Security Strategy, it has worked to make the UK the safest place to live and work online.

This Review of its fifth year looks at some of the key developments and highlights between 1 September 2020 and 31 August 2021. 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.

An accessible version can be found at **ncsc.gov.uk/annual-review-2021**

National Cyber Security Centre
a part of GCHQ

GCHQ

Contents

56

Technology

66

Ecosystem

80

Global Leadership

Ministerial Foreword

The past year has been challenging for us all. During Covid-19 we went online to shop, learn, work, and stay in touch with family and friends more than ever before. With this huge shift has come an equally strong effort by criminal groups to exploit individuals and businesses with scams. From household goods to vaccine appointments, there have been few avenues criminals have not tried to exploit.

Throughout, the NCSC has delivered real-world impact across the UK and internationally. From protecting our most critical services, building NHS resilience and securing vaccine supply, to supporting individuals and stopping opportunistic cyber criminals, to working with like-minded international partners at the G7 and NATO on the most pressing cyber issues, the NCSC continues to lead the way in seeking to make the UK the safest place to live and work online.

This year's annual review demonstrates the incredible work and commitment of the NCSC to tackle these threats, strengthen the UK's cyber ecosystem and bolster our cyber security. Yet it also recognises there remains much more to do in particular to grow skills. This year also marks the culmination of the 5-year National Cyber Security Strategy. As we look back, this government and the NCSC can be proud of its achievements in delivering ambitious, world leading policies and services to protect the UK in cyberspace since 2016.

However, cyberspace is continually evolving. As technology and the way people use it changes, it is vital that cyber remains a priority. The UK must be ready to face these challenges; be more resilient and prepared to compete as well as co-operate. This is why we are taking a new, comprehensive approach to strengthen our position as a responsible and democratic cyber power. The new National Cyber Strategy (NCS) will help chart the UK's course through the cyber age, broadening the scope beyond cyber security to consider the full range of our cyber capabilities and our approach to cyberspace, and giving greater weight to the underpinning technologies and the international environment.

The NCS will take a whole of society approach to cyber, which is underpinned by our values and alliances. Government, industry and the public, in partnership, have an important role in helping make the UK and the lives and livelihoods of its people resilient to the threats, and ready for the opportunities ahead.

The Rt Hon Steve Barclay, MP.
Chancellor of the Duchy of Lancaster
and Minister for the Cabinet Office

CEO Foreword

I am delighted to present the fifth Annual Review of the National Cyber Security Centre, a part of GCHQ. Since becoming the organisation's Chief Executive Officer in October 2020, I have been immensely proud of the work the NCSC has done – and this review reflects an impressive year of delivery.

Over the last 12 months, the NCSC has played a key role in managing significant events and taken action to make the UK a safer place to live and work online. A particular highlight has been the work that the NCSC did to support the Covid-19 vaccine roll out. The NCSC dealt with 777 incidents – an increase on last year – of which 20% were linked to the health sector and vaccines.

One of the trends that the NCSC has seen over the last year was a worrying growth in criminal groups using ransomware to extort organisations. In my view it is now the most immediate cyber security threat to UK businesses and one that I think should be higher on the boardroom agenda.

An international supply-chain data breach emanating from a compromise of SolarWinds was one of the most significant incidents that the NCSC dealt with over the last year. This attack involved one of the world's most popular IT system management platforms being breached by the Russian Foreign Intelligence Service and is an important reminder of the need for organisations to be resilient if one of their suppliers is affected.

But we haven't just spent the last year simply defending against attacks – the NCSC has also taken proactive steps that will make our country thrive in the digital age more safely in the decades to come.

We have continued to roll out the NCSC's Active Cyber Defence Services. This included launching the Early Warning Service, to alert organisations to emerging threats, and the increasing success of the Suspicious Email Reporting Service, which allows the public to report potential scams. The latter is run in partnership with the City of London Police, and since its launch in April 2020 has received more than 7.25 million reports from the public, with almost 60,000 scams taken down as a result.

A big part of the NCSC's mission involves sharing and collaborating with organisations and the public. In the last year we have worked with a range of sectors – from education to farming, sport to Critical National Infrastructure – to provide bespoke advice on becoming more resilient. And we also launched GCHQ's first TV advertising campaign – directly engaging the British public with advice on how they can increase their cyber security.

I would like to thank everybody who has helped to make the UK as safe from cyber threats as possible over the last year. It is truly a team effort between the NCSC, government, law enforcement, business and the public that helps to ensure all of the UK can make the most of the digital age and the opportunities it offers us all.

Lindy Cameron, CEO of the National Cyber Security Centre

National Cyber Security Centre
a part of GCHQ

NCSC Overview and Year Five highlights

- The NCSC was established in 2016 to meet the need for a single focal point in government for cyber security, to improve our national defences and make the UK the safest place to live and work online.
- In the last 12 months, much of our work has focused on surging resources to protect the UK's response to the Covid-19 response.
- Our pioneering Active Cyber Defence programme has taken down 2.3 million cyber-enabled commodity campaigns – including 442 phishing campaigns using NHS branding and 80 illegitimate NHS apps hosted and available to download outside of official app stores.
- When attacks have got through, we have offered support to 777 significant incidents– up from 723 the previous year – with around 20% of organisations supported linked to the health sector and vaccines.
- For example, we helped the University of Oxford's Covid-19 vaccine researchers protect themselves from an attempted ransomware attempt with the potential to cause significant disruption to the UK's pandemic response.
- Our Suspicious Email Reporting Service has received 5.4 million reports from the public of potentially malicious material – leading to the removal of more than 50,500 scams and more than 90,100 malicious URLs.
- Up to 3 million additional key workers were protected from unintentionally accessing malicious domains through our Protective Domain Name System service.

  This included over 1,000 new organisations within the Health and Social Care sector.
- Of course, our work hasn't just been about the pandemic this year. We have engaged with around 5,000 organisations and issued guidance and threat assessments to 80 companies and 14 universities.
- In our attempt to increase the pipeline of skills and diversity of the cyber security profession, we have introduced more than 56,000 11-to-17 year olds to the world of tech and cyber security through our CyberFirst programme – including around 6,500 pupils from 600 schools to the CyberFirst Girls competition.

Sir Jeremy Fleming

Life today is dependent on technology. The hard definition between online and the real world is blurring. This Annual Review shows why world class cyber security, enabled by the expertise of the NCSC as part of GCHQ, continues to be vital to the UK's safety and prosperity.

The cyber threat continues to grow. The past year saw the cyber attack on Microsoft, linked to a Chinese state-backed threat actor, and the SolarWinds attack, attributed to Russia's Foreign Intelligence Service. Two of the most serious global cyber incidents we've seen in recent years.

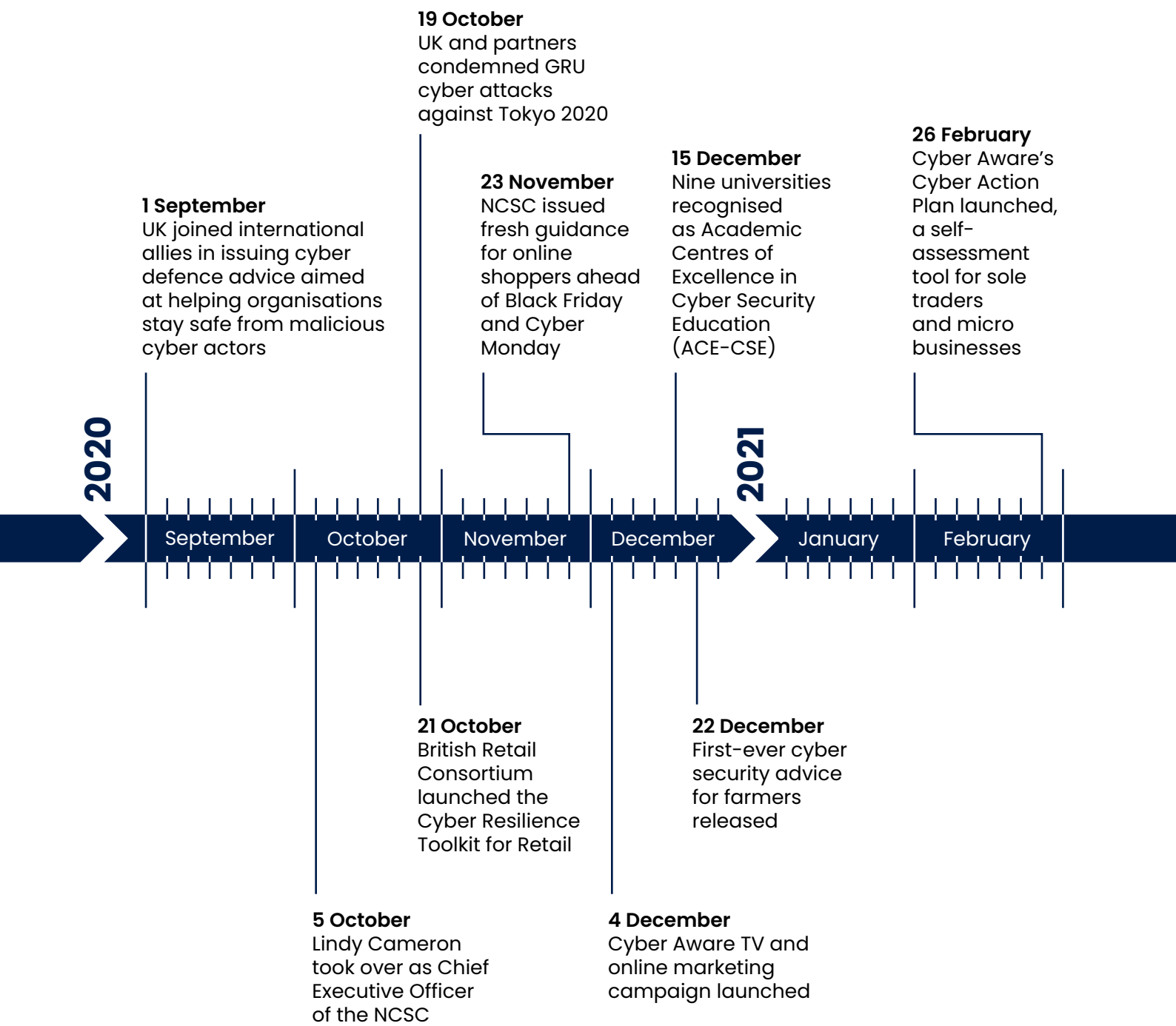
In the UK there was an increase in the scale and severity of ransomware attacks, targeting all sectors from businesses to public services. In response, the NCSC has identified and mitigated numerous threats, whether committed by sophisticated state actors, organised criminal groups or lone offenders.

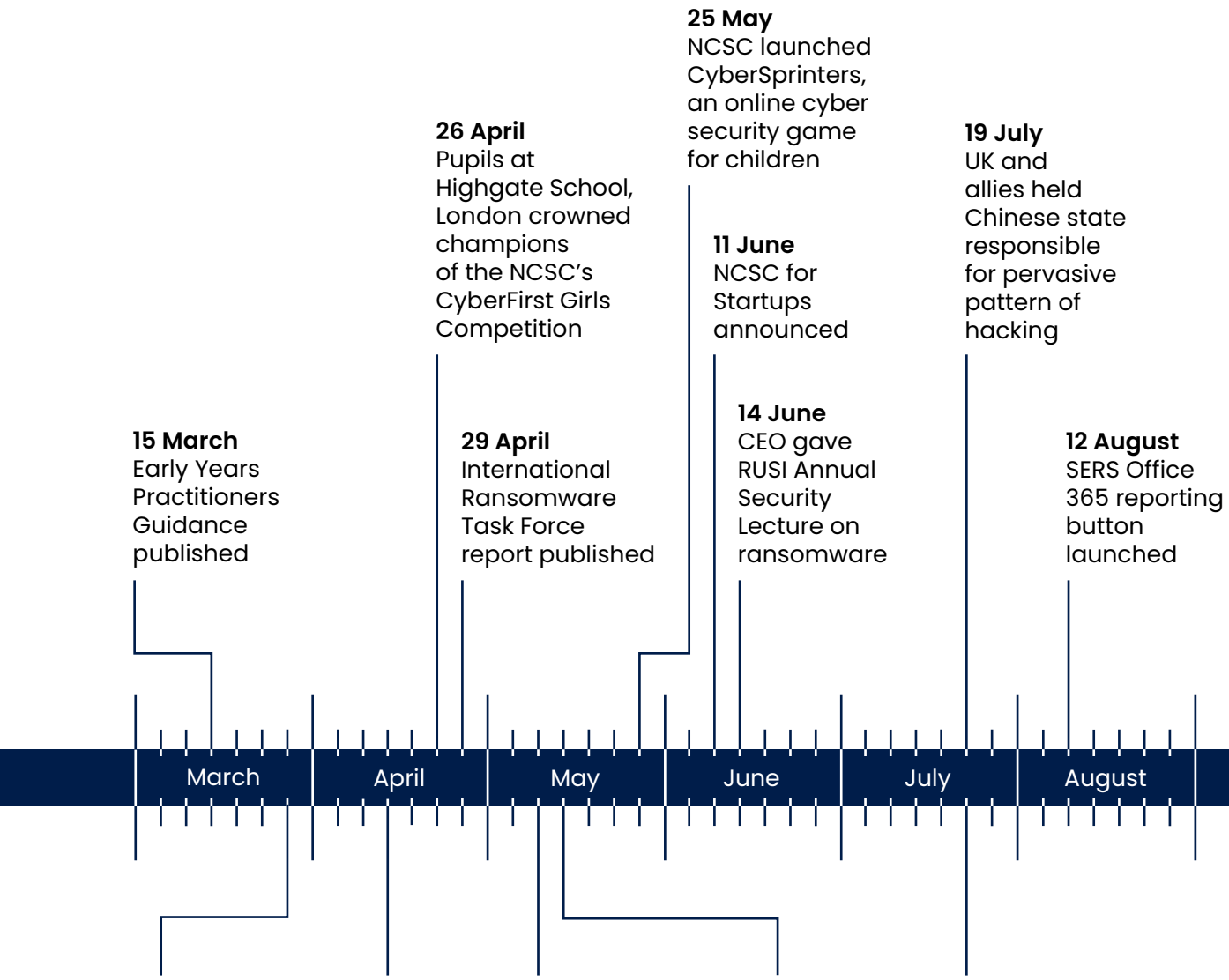
Of course, coronavirus continues to shape what we see. Cyber criminals are still exploiting the pandemic, while hostile states shifted their cyber operations to steal vaccine and medical research. The NCSC worked across the four nations to protect those involved in the UK's response, including the NHS, medical research and the vaccine supply chain. The NCSC's impact has been substantial and far reaching at a time of global crisis.

The Government's investment in cyber security means we know much more about the changing threats the country faces today than we did five years ago, when the NCSC was set up. And we are looking ahead too. We can see technology leadership is shifting eastwards. The key technology we will rely on for future prosperity and security won't necessarily have democratic values at its core. We will work with partners around the world to help the UK and allies face this moment of reckoning.

Sir Jeremy Fleming, Director GCHQ

NCSC Timeline 2020-2021





15 March
Early Years Practitioners Guidance published

26 March
Lindy Cameron warned, in her inaugural speech as CEO, that cyber security is still not taken as seriously as it should be, and is not embedded in boardroom thinking.

26 April
Pupils at Highgate School, London crowned champions of the NCSC's CyberFirst Girls Competition

29 April
International Ransomware Task Force report published

15 April
UK and US attributed SolarWinds compromise to Russia-based actions.

25 May
NCSC launched CyberSprinters, an online cyber security game for children

10 May
Fourth Active Cyber Defence report published

11-12 May
CYBERUK 2021 took place online

11 May
NCSC's Early Warning service launched, a free service designed to help organisations

11 June
NCSC for Startups announced

14 June
CEO gave RUSI Annual Security Lecture on ransomware

11 May
10 Steps to Cyber Security guidance published

12 May
Cyber Essentials Readiness Tool launched a free online resource that helps organisations prepare for certification

19 July
UK and allies held Chinese state responsible for pervasive pattern of hacking

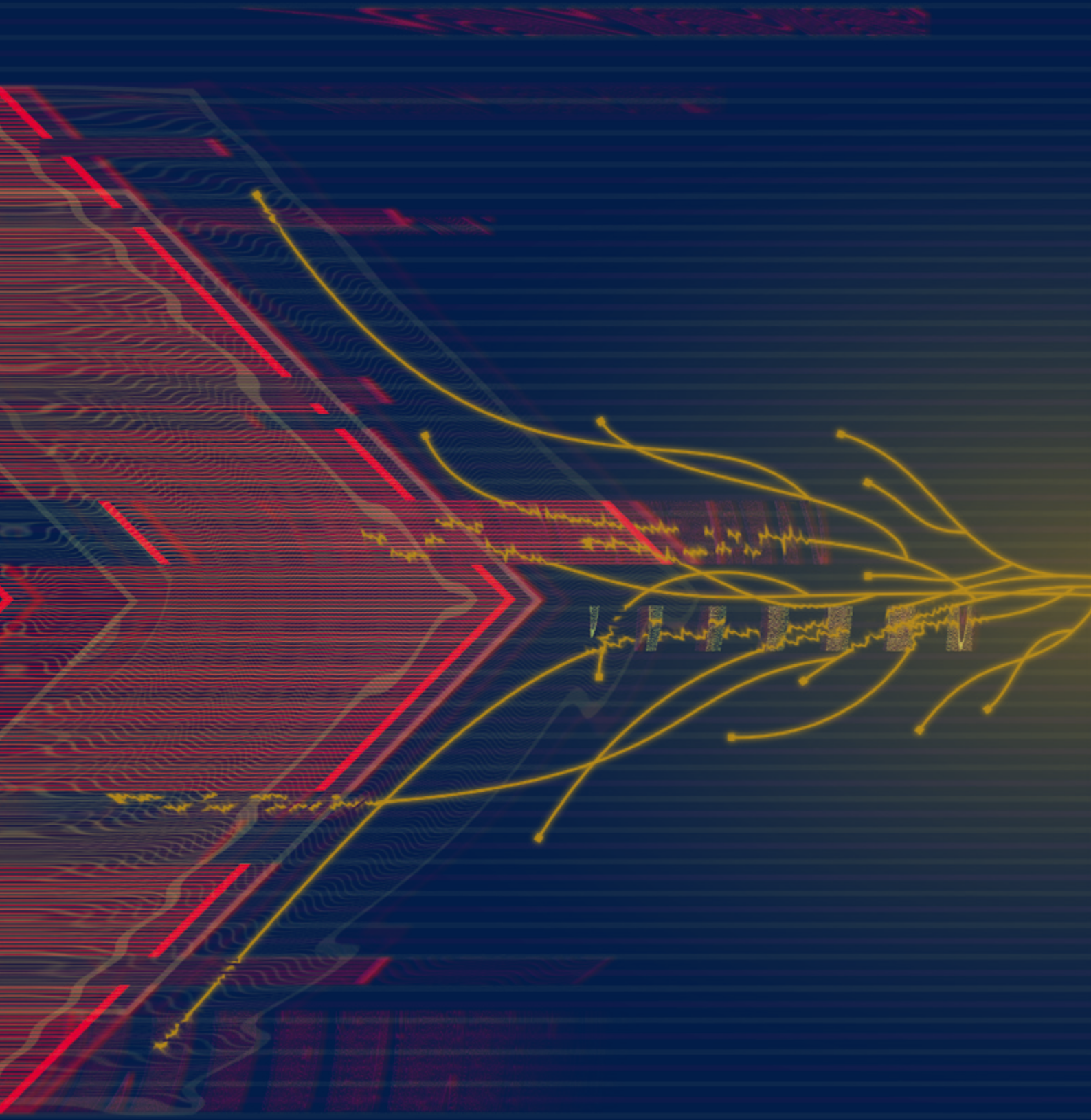
19-22 July
CEO made first international visit at Tel Aviv Cyber Week

20 July
Report published by the Oversight Board of the Huawei Cyber Security Evaluation Centre (HCSEC)

12 August
SERS Office 365 reporting button launched

The Threat

How the NCSC assesses, responds to, disrupts and deters cyber threats



The Threat

The cyber threat to the UK and its allies continued to grow and evolve this year: from indiscriminate phishing scams against mass victims, to ransomware attacks against public and private organisations, to targeted hostile acts against critical national infrastructure and government.

While the threats came from a range of actors using an array of methods, they had one thing in common; they led to real-world impact. Life savings were stolen, critical and sensitive data was compromised, healthcare and public services were disrupted, and food and energy supplies were affected.

In the past 12 months the NCSC continued, in partnership with law enforcement, to monitor, counter and mitigate the threat, whether committed by sophisticated state actors, organised criminal groups or low-level offenders. This section describes the key threats, who was behind them and how the NCSC responded.

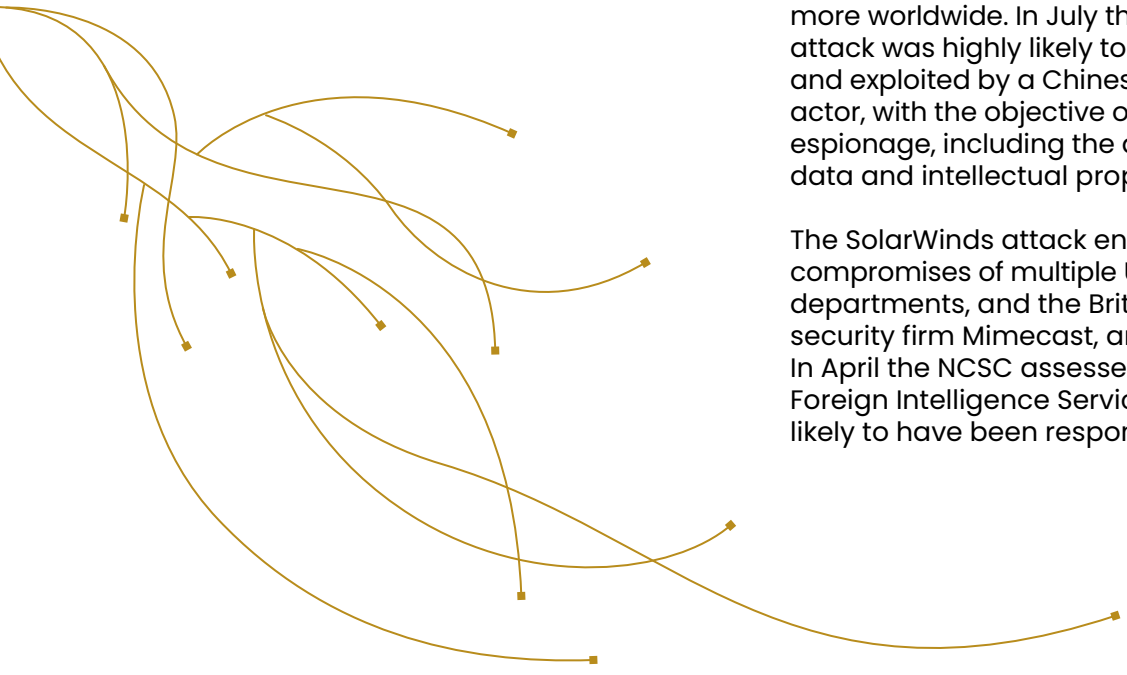
Covid-19 continued to shape the cyber security landscape. Cyber criminals continued to exploit the pandemic as an opportunity, while hostile states shifted their cyber operations to steal vaccine and medical research, and to undermine other nations already hampered by the crisis. The pandemic has also brought about an acceleration in digitisation, with businesses and local government increasingly moving services online and essential services relying ever more on cloud IT provision. This has broadened the surface area for attacks and has often made cyber security more challenging for organisations.

In response the NCSC built on the experiences of last year in protecting sectors responding to the pandemic, including the NHS (across all four nations), medical research, vaccine manufacturers and distributors, encouraging them to take up the services available to respond to threats to their security.

The compromise of the software company SolarWinds and the exploitation of Microsoft Exchange Servers highlighted the threat from **supply chain attacks**. These sophisticated attacks, which saw actors target less-secure elements - such as managed service providers or commercial software platforms - in the supply chain of economic, government and national security institutions were two of the most serious cyber intrusions ever observed by the NCSC.

In March 2021, Microsoft announced that four zero-day vulnerabilities in Microsoft Exchange Servers were being actively exploited with at least 30,000 organisations reportedly compromised in the US alone, affecting many more worldwide. In July the NCSC assessed this attack was highly likely to have been initiated and exploited by a Chinese state-backed threat actor, with the objective of enabling large-scale espionage, including the acquisition of personal data and intellectual property.

The SolarWinds attack enabled the onward compromises of multiple US government departments, and the British cloud and email security firm Mimecast, among other victims. In April the NCSC assessed that Russia's Foreign Intelligence Service (SVR) was highly likely to have been responsible for the attack.



Ransomware became the most significant cyber threat facing the UK this year. Due to the likely impact of a successful attack on essential services or critical national infrastructure, it was assessed as potentially harmful as state-sponsored espionage.

In 2020 the NCSC observed the evolving model of criminals exfiltrating data before encrypting victim networks; data which they then threatened to leak unless the ransom was paid (known as double extortion).

Ransomware gained increased public attention following attacks on Colonial Pipeline in the US, which supplied fuel to the East Coast, and against the Health Service Executive in Ireland. In the UK there was an increase in the scale and severity of ransomware attacks. Hackney Borough Council suffered significant disruption to services – leading to IT systems being down for months and property purchases within the borough delayed. Attacks this year were across the economy, targeting businesses, charities, the legal profession and public services in the education, local government and health sectors.

Among other ransomware incidents investigated was a major attack on the American software firm Kaseya. In July, the NCSC helped to identify and support British victims after the Florida-based company was infiltrated by a hacking group, which seized troves of data and demanded $70m (£51.5m) in cryptocurrency for its return.

The NCSC welcomed international efforts in tackling ransomware when it was discussed at the G7 meeting of world leaders in Cornwall, underlining the need for co-ordinated multilateral attention.

Global threat actors

The NCSC continued its work with global partners to detect and disrupt shared threats, the most consistent of these emanating from Russia and China. In addition to the direct cyber security threats posed by the Russian state, it became clear that many of the organised crime gangs launching ransomware attacks against western targets were based in Russia.

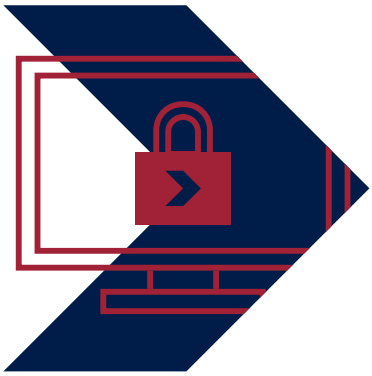
China remained a highly sophisticated actor in cyberspace with increasing ambition to project its influence beyond its borders and a proven interest in the UK's commercial secrets. How China evolves in the next decade will probably be the single biggest driver of the UK's future cyber security.

While less sophisticated than Russia and China, Iran and North Korea continued to use digital intrusions to achieve their objectives, including through theft and sabotage.

"We will work with the FCDO to put cyber power at the heart of the UK's foreign policy agenda, strengthening our collective security, ensuring our international commercial competitive advantage and shaping the debate on the future of cyberspace and the internet.

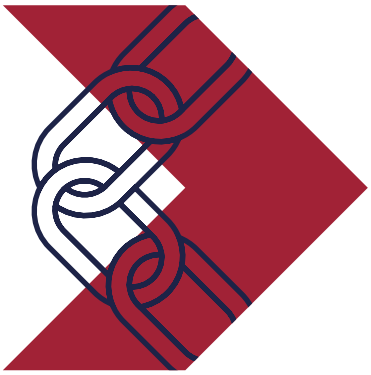
"We will need to reinforce our core alliances and lead a compelling campaign aimed at middle-ground countries to build stronger coalitions for deterrence and counter the spread of digital authoritarianism. This will involve better connecting our overseas influence to our domestic strengths, leveraging our operational and strategic communications expertise, thought leadership, trading relationships and industrial partnerships as a force for good."

Lindy Cameron, NCSC's CEO



Cyber Threat 2021

Ransomware and **supply chains** as an attack vector were prominent in the UK's cyber threat landscape.



Double Extortion
In 2020, criminals sought to exfiltrate data before encrypting victim networks, data which they then threatened to leak unless the ransom was paid (so-called double extortion). **This has now become routine.**

Supply chains - in which managed service providers operate - are based on trusted relationships. Compromises provided access to better-protected targets in multiple sectors.

Ransomware gained increasing public notoriety through attacks against:

Colonial Pipeline, US

Health Service Executive, Ireland

In the UK, education has been among the top sectors targeted.

Ransomware threat of leaking stolen data is **almost certain** to grow. Further UK victims of this dual-crime are **highly likely.**

Supply chain incidents highlight the viability, effectiveness and global reach of supply chain operations as a means of compromising comparatively well-defended targets. Further such operations are **almost certain** over the next 12 months.

This threat is not new but **SolarWinds** and **Microsoft Exchange Servers** were particularly high-impact operations.

The SolarWinds compromise enabled onward access to multiple US government departments, Mimecast (the UK cloud and email security firm) and many other victims. NCSC assesses that Russia's Foreign Intelligence Service (SVR) was highly likely responsible.

Open source reporting indicates that 30,000 organisations were compromised in the US alone from zero-day vulnerabilities in Microsoft Exchange Servers. NCSC assesses that it was highly likely initiated and exploited by a Chinese State-backed actor. It was highly likely in support of a large-scale espionage operation.

Visualisation of the core threat in 2021, which focused on ransomware and supply chains

Real-World Impact

The real-world impact of these attacks in the UK and around the world was stark: food supplies were affected, local fuel prices increased, citizens were denied access to public services, at-risk children's details were lost and the costs to businesses and public funds ran into hundreds of millions of pounds.

In July the Irish Health Service Executive announced the recovery costs from an attack in May would be $600m (£442m), while Hackney Borough Council estimated in February it would cost approximately £10m to recover from a cyber breach in 2020.

As part of the wider intelligence community, the NCSC has a role in identifying threat actors, and attributing – in partnership with the government – their malign activity. Attribution continued to be an important part of cyber deterrence, with perpetrators identified and their actions exposed.

Due to the interconnected nature of cyberspace most major attacks carried out overseas caused an impact in the UK. The NCSC supported those organisations affected with guidance and tools to help prevent compromise, or to recover systems and services.

While high-profile ransomware attacks attracted public attention, it was not just global corporations or Critical National Infrastructure (CNI) affected by the cyber threat this year. According to the DCMS Cyber Security Breaches Survey published in March, 39% of all UK businesses (that's 2.3m) reported a cyber breach or attack in 2020/21, compounding an already difficult year for many SMEs.

Image credit: ink drop - stock.adobe.com

Supply Chain Attacks

SolarWinds

In April 2021 the NCSC, together with its security counterparts in the US, revealed for the first time that Russia's Foreign Intelligence Service (SVR) was behind one of the most serious cyber intrusions of recent times, an attack on the popular SolarWinds IT management platform.

This major attribution came five months after the first warning by the NCSC that SolarWinds had been compromised and could be used for further attacks on connected systems.

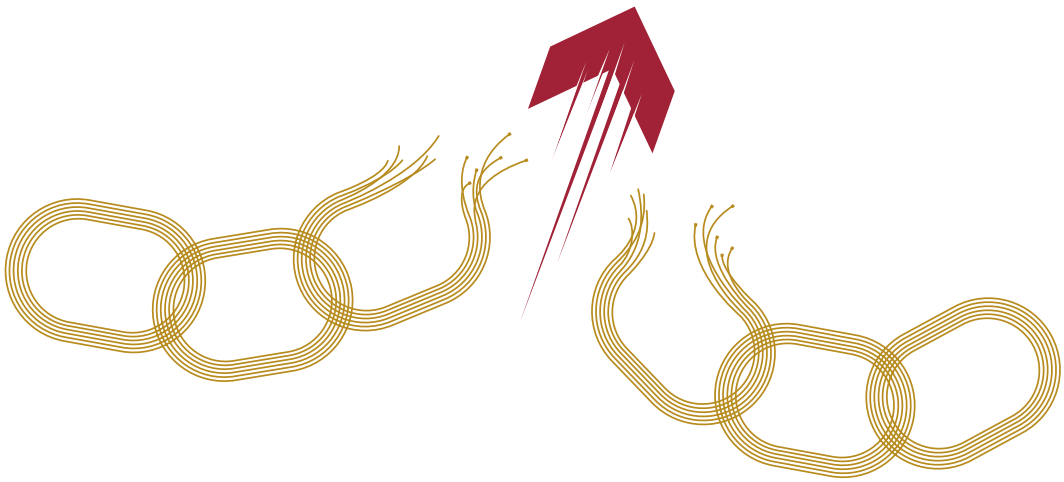
A US cybersecurity firm, FireEye, found that an attacker had been able to add a malicious modification to SolarWinds Orion products which allowed them to send administrator-level commands to any affected installation. The NCSC, working with colleagues in the US and across industry, investigated the impact of this incident.

When the attack became apparent, NCSC analysts used data from ACD services to estimate the extent of the incident, inform decision-makers in government, and support affected organisations.

The Protective Domain Name System allowed the NCSC to immediately identify historical evidence of compromise of customer organisations, while the Host Based Capability service provided the ability to build a more detailed view of affected devices and activity on customer networks.

The NCSC was able to identify which organisations and sectors were affected to help further the investigation, and to help make contact and provide technical advice and support.

Investigators assessed that it was highly likely that the SVR was responsible for the attack and subsequent targeting. At the same time a technical advisory with mitigation advice was issued by the NCSC, in partnership with the US National Security Agency (NSA), Department of Homeland Security's Cybersecurity Infrastructure Security Agency (CISA) and the FBI.



Supply Chain Attacks

Microsoft Exchange

Research and analysis carried out by the NCSC enabled the UK Government in July 2021 to call out Chinese state-backed actors for gaining access to computer networks around the world via Microsoft Exchange servers in what is the most significant and widespread cyber intrusion against the UK and allies ever observed by the NCSC.

NCSC experts assessed the attack was highly likely to enable large-scale espionage, including acquiring personally identifiable information and intellectual property. It was reported that at least 30,000 organisations were compromised in the US alone, with many more affected worldwide.

As part of a UK Government response, the NCSC issued tailored advice to over 70 affected organisations to enable them to mitigate the effects of the compromise.

The NCSC used its technical understanding of the Chinese cyber threat to inform the attribution and the subsequent multi-lateral efforts when the UK joined 38 partners, including the Five Eyes, NATO, the EU and Japan, to attribute variously HAFNIUM, APT31 and/or APT 40 to the Chinese state. Acts included the targeting of maritime industries and naval defence contractors in the US and Europe, and targeting of foreign democratic institutions, including the Finnish parliament in 2020.

"The attack on Microsoft Exchange servers was another serious example of a malicious act by Chinese state-backed actors in cyberspace. This kind of behaviour is completely unacceptable and alongside our partners we will not hesitate to call it out when we see it."

Paul Chichester, NCSC's Director of Operations

Incident Management

While the NCSC does all it can to prevent attacks in the first place, it works continuously with its partners to respond to breaches, while helping victims to recover. The NCSC's operations and incident response team, which works closely with law enforcement and intelligence partners, handled high volumes of incidents as well as major attacks that affected thousands of victims.

Incident Management response model:

NCSC becomes aware of incident	NCSC triage incident	NCSC support victim	X-HMG coordination	Incident closure & insight sharing
› NCSC's 24/7 incident management function › Incident is reported to NCSC by victim **OR** › Incident is reported to NCSC by partner organisation **OR** › Incident is detected by NCSC	› Initial engagement with the victim to fully understand the incident › Determine if further response merited and a ticket assigned › A preliminary decision on the categorisation of the incident › Determine whether NCSC support is appropriate	› Deliver effective real world response to minimise harm › Facilitate the technical response to an incident, drawing on X-NCSC teams including – Industry partners – Technical specialists – Communications › Work with law enforcement in support of a criminal investigation	› Lead the National Incident Response including liaising with: – Whitehall – Law Enforcement – Industry – international partners › To manage the incident and ensure coherence of response	› Alongside NCSC Resilience team, provide aftercare and inform "Lessons learned" for wider UK resilience › Provide incident insight to inform Whitehall policy › Develop exercising & red teaming to respond effectively to similar incidents in future

It was a record year for incidents dealt with by the NCSC. The team managed 777 incidents, another increase on the previous record, breaking 723 total from last year. NCSC supported the NHS during 8 high severity alerts from April 2020 to March 2021.

This year's total means that since the NCSC commenced operations in 2016, the organisation has co-ordinated the UK's response to a total of 3,305 incidents (annual totals of 590, 557, 658, 723 and 777). Several incidents came onto the NCSC's radar proactively, through the expert work of its threat operations and assessments teams. Many others were raised by victims of malicious cyber activity.

While the NCSC has world-leading capabilities in identifying, confronting and responding to cyber threats and deterring those responsible for them, it is just as important to improve defences to stop attacks getting through in the first place, and when they do, that organisations are better able to recover and limit the impact. The next chapter will describe how the NCSC is helping to create

Ransomware

Ever evolving threat

In the last Annual Review, the NCSC set out how the ransomware model had shifted from not only withholding data but threatening to publish it as well. This year the model has developed further into what is termed Ransomware as a Service, (RaaS) where off-the-shelf malware variants and online credentials are available to other criminals for a one-off payment or a share of profits.

As the business model has become more and more successful, with these groups securing significant ransom payments from large businesses who cannot afford to lose their data to encryption or to suffer the down time while their services are offline, the market for ransomware has become increasingly 'professional'.

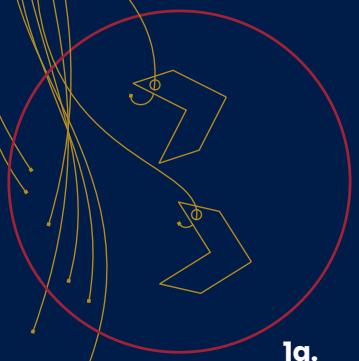
The NCSC has observed that some victims have been offered the services (from the attackers) of a 24/7 help centre to quickly pay the ransom and get back online. Everything is geared to make it as easy as possible to simply pay the ransom and move on.

Organised crime groups spend time conducting in-depth reconnaissance on their targeted victims. They will identify exploitable cyber security weaknesses. They will use spoofing and spearphishing to masquerade as employees to get access to the networks they need. They will look for the business-critical files to encrypt and hold hostage. They may identify embarrassing or sensitive material that they can threaten to leak or sell to others. And they may even research to see if a potential victim's insurance covers the payment of ransoms.

This process can be painstaking and lengthy, but it means that, when they are ready to deploy, the effect of ransomware on an unprepared business is brutal. Files are encrypted. Servers go down. Digital phone lines no longer function. Everything comes to a halt and business is stopped in its tracks.

But it's not all bad news. There are many services that organisations can use to protect themselves against ransomware or mitigate the impact of an attack. As well as implementing practical cyber security measures and following advice, an important defence against ransomware is to understand the ever-evolving threat picture and working with others to share information and good practice.

The NCSC's Cyber Security Information Sharing Partnership (CISP) service provides a secure forum where companies and government can collaborate on threat information. CISP, which also gives access to regular sensitive threat reports, is one of many tools available, as can be seen in the next chapter.



1a.

How Active Cyber Defence (ACD) protects against the ever evolving threat of ransomware

1 Preventing ransomware getting in.

The NCSC provides a range of free cyber security tools and services to eligible organisations as part of the Active Cyber Defence (ACD) programme. These initiatives help organisations to find and fix vulnerabilities, manage incidents or automate disruption of cyber attacks. Some of our services are designed primarily for the public sector, whereas others are made available more broadly to private sector or citizens, depending on their applicability and viability.

ACD helps organisations secure aspects of their IT that are frequently exploited to deliver ransomware.

a. We know that phishing and compromise of exposed **Remote Desktop Protocol** ports are the main vectors for ransomware

b. **Mail Check** helps users configure a security protocol called **DMARC** which protects against phishing that involves spoofing their domains. NCSC's **Synthetic DMARC** service does the same for non-existent gov.uk domains.

c. **Web Check** and **Early Warning** scan users' web services for exposed ports, such as port 3389 which is used for **Remote Desktop Protocol**.

d. Another common vector for ransomware is software vulnerabilities, which **HBC**, **Early Warning**, **Web Check**, the **Vulnerability Disclosure Service** and **Vulnerability Disclosure Toolkit** seek to address.

>2 Preventing ransomware working.

ACD helps to disrupt ransomware that makes it through the first line of defence onto an organisation's network.

a. Protective Domain Name System (PDNS) can prevent ransomware from operating by blocking connections to known ransomware domains. The deny-list is drawn from a range of sources including commercial feeds and NCSC intelligence.

b. The Suspicious Email Reporting Service (SERS) allows members of the public to report suspicious emails to the NCSC. Any ransomware domains that are identified by SERS are passed to the Takedown service. The Takedown service also receives feeds of malicious domains from other sources and it sends notices requesting the removal of malicious domains to the companies that host them. The Takedown service also adds the malicious domains to safe browsing lists so modern browsers block access to them. As part of our Routing and Signalling work, the SMS SenderID Protective Registry is similar to PDNS but for SMS.

c. The Exercise in a Box service helps organisations practice their response to cyber security scenarios and incidents. These exercises help organisations prepare to limit the impact of cyber attacks, including ransomware.

>3 Enabling investigation and incident response.

ACD provides data and tools to investigate suspected ransomware and respond to it.

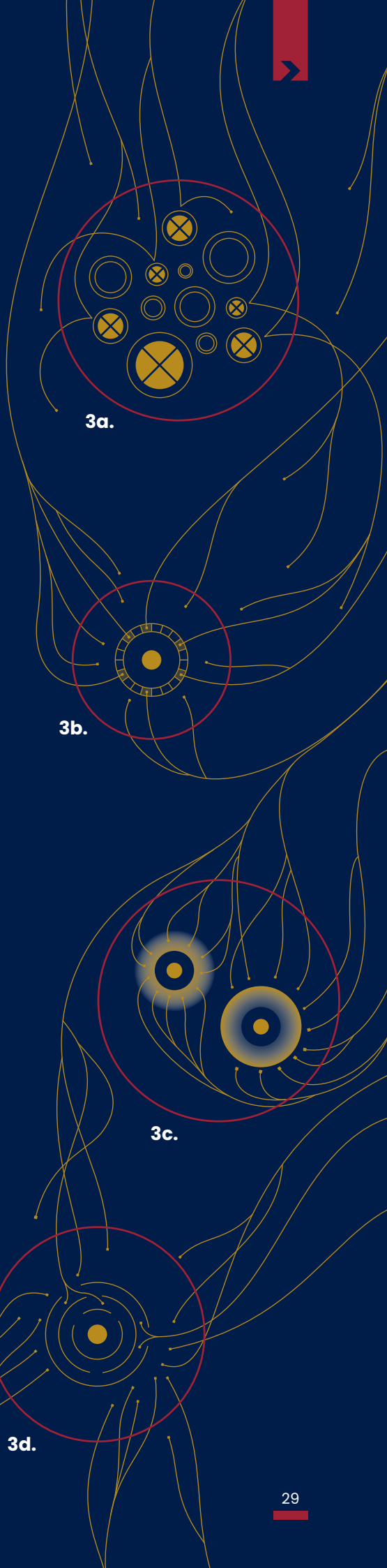
a. Even when a ransomware domain is unknown to the PDNS deny-list at the time of the suspicious query, the service records the fact a customer organisation attempted to connect to the domain. These records can be used to identify the presence of ransomware in an organisation after the event, once the domain is identified as suspicious.

b. HBC can detect threats on customer networks. The software agent is installed widely on OFFICIAL government devices and sends technical metadata to NCSC's expert analysts who use specialist techniques to identify suspicious activity.

c. HBC and PDNS are complementary. PDNS provides an estimate of which organisations might be affected by ransomware, whereas HBC is well placed to conduct more detailed investigations into activity on specific devices.

d. Early Warning can identify active compromises on customer networks by mapping threat intelligence from a variety of sources to customer IP ranges, ASNs and domain names. The service alerts users to incidents, suspicious network activity, vulnerabilities, and undesirable open ports.

› *For more information about our Active Cyber Defence programme, please read on to p36.*



Ransomware

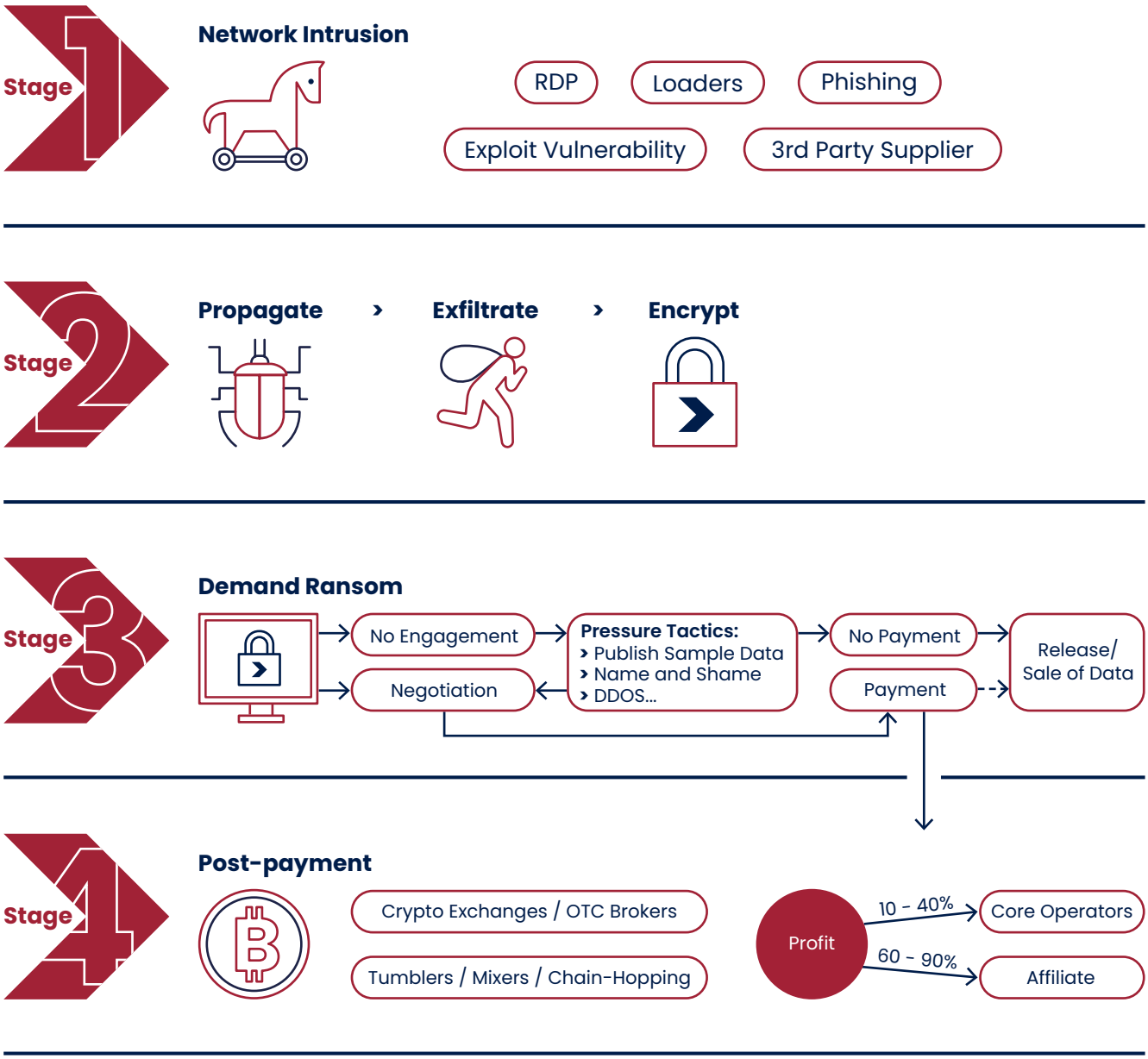
Threat methodology

While there are numerous entry points into a system, device or network, the NCSC has observed threat actors have been increasingly exploiting vulnerabilities in virtual private networks, unpatched software and using phishing emails. The most commonly used attack vectors by ransomware actors targeting the UK include:

- RDP: Remote desktop protocol attacks are the most commonly exploited remote access tools used by ransomware hackers. Hackers use insecure RDP configurations collected through phishing attacks, data breaches or credential harvesting to gain initial access to the victim's environment.
- VPN: Since the shift in remote learning and working since the pandemic began, threat actors have been exploiting vulnerabilities present in Virtual Private Networks to take over the remote access.
- Unpatched devices: Attackers are targeting unpatched software and hardware devices to gain access to the victim's network. One example of this is the vulnerabilities in Microsoft Exchange Server that are known to have been used by persistent threat groups.

The NCSC released tools and advice designed to help organisations prevent ransomware attacks. These included guidance on mitigating ransomware attacks; a tool called Early Warning Service, designed to help organisations facing cyber attacks on their network; training for school staff, and a range of Active Cyber Defence services including Web Check – a tool that provides website configuration and vulnerability scanning services. This report will set out how the NCSC is bolstering the resilience of the UK in the next chapter.

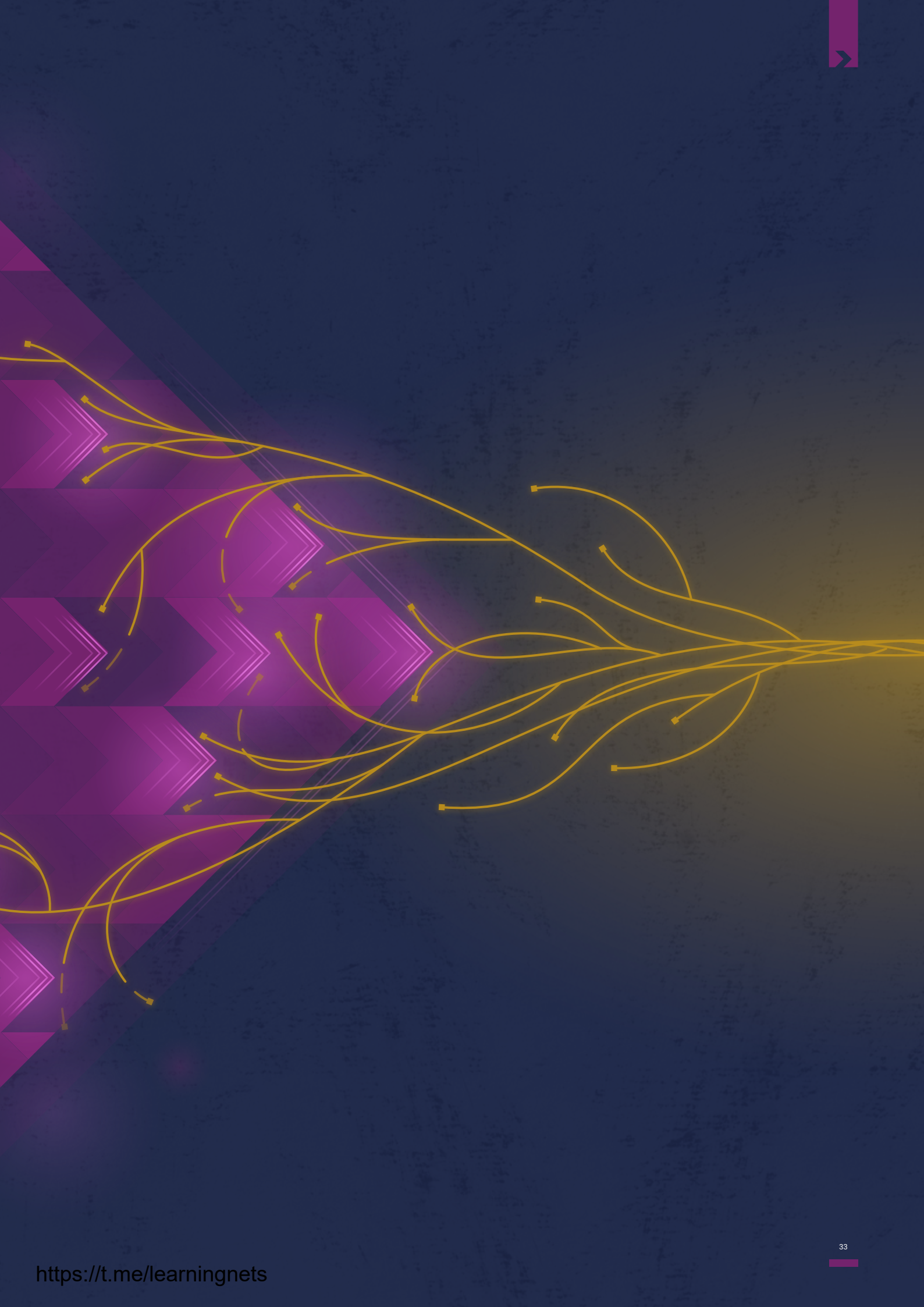
In the first four months of 2021, the NCSC handled the same number of ransomware incidents as for the whole of 2020 – which was itself a number more than three times greater than in 2019.



The four stages of a ransomware attack

Resilience

How the NCSC is building a cyber resilient UK



Resilience

One of the NCSC's most important priorities this year was to increase the resilience of the UK against cyber threats and strengthening the systems pivotal to the nation's response to Covid-19. Chapter one of this review sets out some of the NCSC's actions to identify and assess those threats and how it managed incidents and deterred and disrupted hostile actors.

This chapter describes how the NCSC engaged and advised sectors, developed new tools and services, and extended existing ones, to help central, devolved and local governments, businesses, organisations and citizens be more resilient to the threat and better able to respond and recover if attacks got through.

Businesses and organisations, as well as local government and the public sector, are increasingly dependent on digital technologies. These technologies help to drive growth and innovation across the economy but create new risks and challenges. Despite good progress made in recent years, many organisations are still not managing their cyber risk effectively, which is why the NCSC continued to work to ensure sectors were more secure and resilient to cyber threats.

As the UK's technical authority for cyber security, a key part of the NCSC's work is to issue advisories and strategic warnings – with accompanying guidance - to help organisations better understand the risk and threat, and the actions they need to take to increase resilience against them.

Key advisories and interventions

September 2020 – The NCSC and its Five Eyes partners issued a joint advisory to help organisations stay safe from malicious cyber actors. It highlighted technical approaches for sectors – including those which protect critical national infrastructure – to uncover malicious activity and mitigation steps based on best practice.

October 2020 – The NCSC published updated guidance for the UK health sector following a US advisory on Ryuk ransomware attacks against the US health sector as cyber criminals continued to exploit the pandemic.

December 2020 – The NCSC confirmed it was working to assess the impact of the SolarWinds compromise and published guidance for Orion product users, urging them to follow advice in recently published FireEye and Microsoft blogs.

March 2021 - Organisations were advised to install the latest Microsoft Exchange Server updates, as a matter of urgency, to avoid compromise by an increasing range of threat actors and to reduce the risk of future ransomware and other malware infections. This followed Microsoft's warning of large-scale exploitation of unpatched vulnerabilities and issued multiple security updates for the affected servers.

March 2021 – In her inaugural speech as CEO of the NCSC, Lindy Cameron warned against complacency in the boardroom while outlining future cyber risks. Ms Cameron called on CEOs and boards to embed cyber security in their thinking and position digital literacy as non-negotiable as financial or legal literacy.

June 2021 – Delivering the RUSI Annual Security Lecture, CEO Lindy Cameron warned that ransomware was now the key cyber threat facing the UK and allies and had brought real-world impact in ways not seen before. She called for a whole of society approach and partnerships to address this challenge and that all organisations now needed to take the ransomware threat seriously.

July 2021 - The NCSC and US and Australian counterparts published a joint advisory to address the top 30 vulnerabilities routinely exploited by malicious actors in 2020 globally, and shared details of Common Vulnerabilities and Exposures (CVEs) being widely exploited in 2021.

Active Cyber Defence

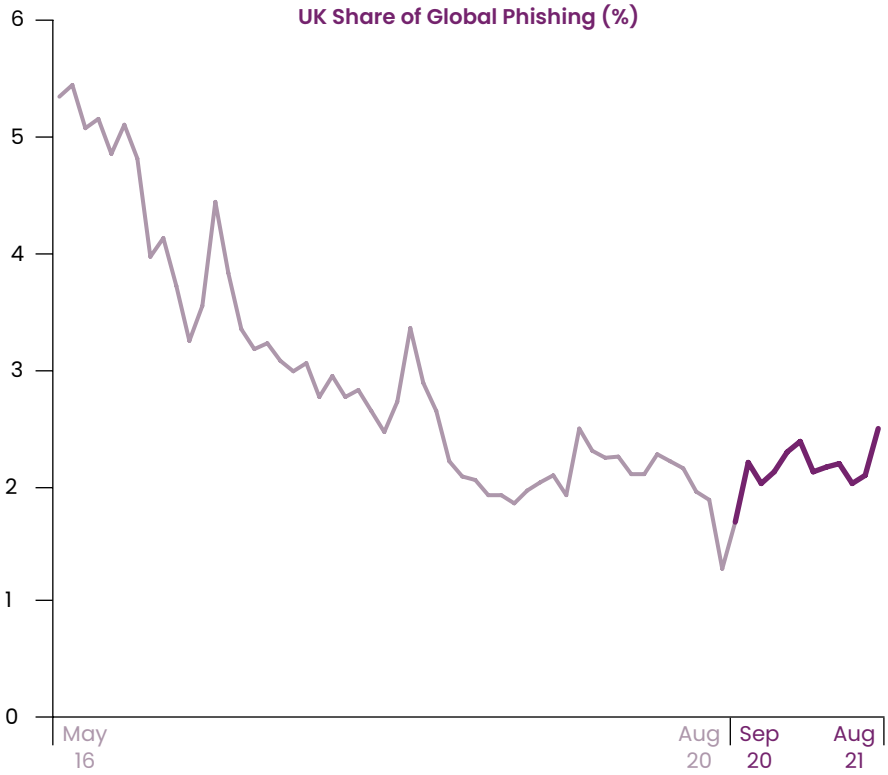
Building Resilience at Scale

The Active Cyber Defence (ACD) programme is one of the NCSC's most successful ways to help bring about a real-world, positive impact against threats. The programme seeks to reduce high-volume cyber attacks, such as malware, ever reaching UK citizens and aims to remove the burden of action from the user.

The ACD programme's core services include Mail Check, Web Check, Protective DNS, Exercise in a Box, the Suspicious Email Reporting Service, and the Takedown Service.

Active Cyber Defence Services

Takedown Service
Finds malicious sites and sends notifications to the host or owner to get them removed from the internet before significant harm can be done. The NCSC centrally manages the service, so departments automatically benefit without having to sign up. This year, the UK's share of global phishing has remained consistent at approximately 2% due to this service.

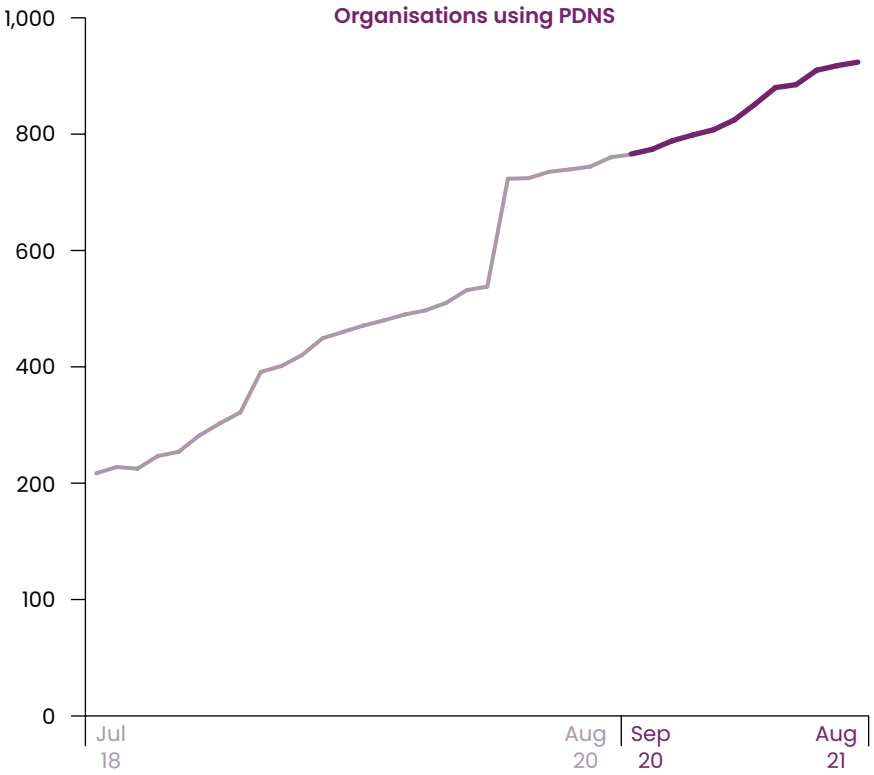


This year the Takedown Service enabled the NCSC to remove a total of 2.3 million cyber-enabled commodity campaigns, including:

- **13,000 phishing campaigns** which were disguised as coming from the UK Government
- **442 phishing campaigns** which used NHS branding, compared to 105 in the same period in last year's report
- **80 instances** of NHS apps (unofficial mirrors) hosted and available for download outside of the official Apple and Google app stores.

Mail Check
Helps organisations secure their email, in particular standards that prevent criminals from spoofing their email domains (DMARC), encryption-in-transit (TLS and MTA-STS). This year the number of public sector domains using DMARC has increased by 38% (from 3,097 to 4,273).

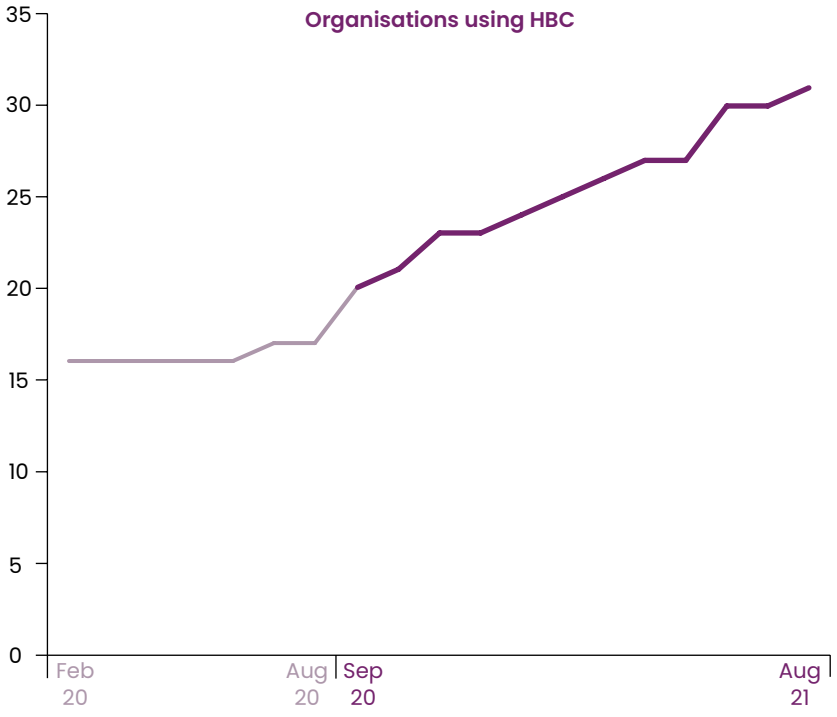
Web Check
Helps owners of public sector websites to identify and fix common security issues, making sites in the UK a less attractive target to attackers. This year Web Check has resolved 8,746 distinct urgent issues.



Protective Domain Name System (PDNS)
PDNS prevents users from accessing domains or IPs that are known to contain malicious content and stops malware already on a network from calling home. This year, the number of organisations using PDNS has risen 20% (from 766 to 925).

There was a significant increase in customer onboarding in March 2020, when we extended PDNS to Healthcare organisations, and vaccine development and supply chain organisations.

Routing and Signalling
Fixing the underlying infrastructure protocols on which the internet and telephony systems are based: the Border Gateway Protocol (BGP) and the Signalling System No. 7 (SS7). This includes setting up initiatives such as the SMS SenderID Protective Registry, which helps organisations protect their brand from abuse in SMS phishing campaigns.

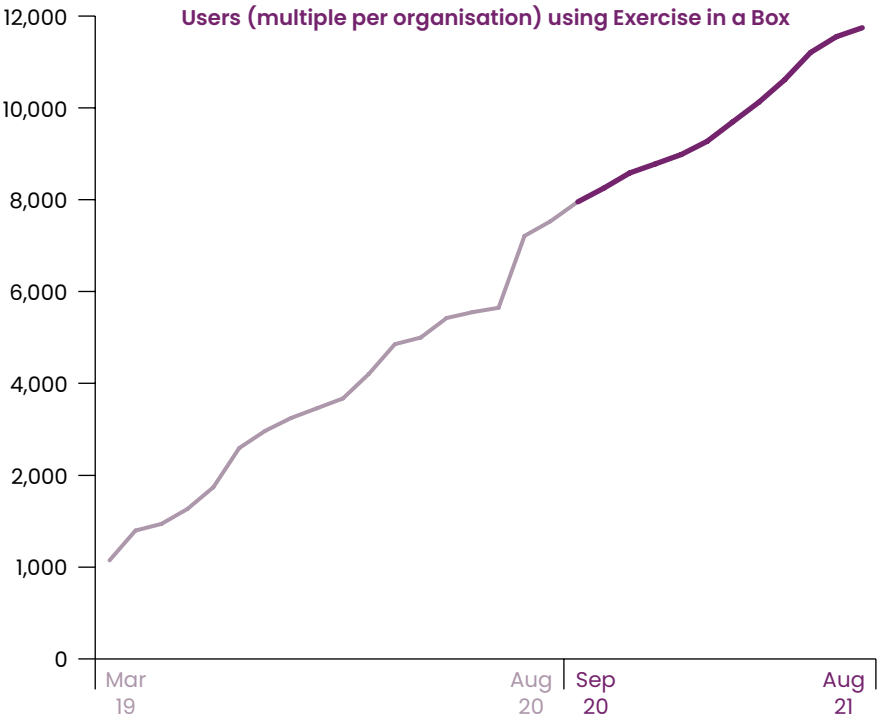


Host Based Capability
Advanced NCSC threat detection capability that can be deployed to detect threats on an organisation's network. This year, there has been a 50% rise in organisations using this service (from 20 to 31).

Vulnerability Disclosure
Services based around making it easier to report, manage and remediate vulnerabilities in government and other key services. This year 13 Government departments launched dedicated vulnerability disclosure programs with the aid of our Vulnerability Disclosure Pilot. In addition, the Vulnerability Reporting Service helped to remediate over 400 vulnerabilities.

NCSC Observatory
Generating data-driven insights to underpin the NCSC's research and strategy, which includes supporting the other ACD services. DNS Insights (DNSI), part of the the NCSC Observatory, now processes over 2.1 billion DNS requests per day, up from 1 billion in October 2020

Suspicious Email Reporting Service
Allows the public to report phishing or suspicious emails they receive in their inboxes. The service analyses the emails for links to malicious sites, and then seeks to remove those sites from the internet to prevent the harm from spreading. The service has now received more than 5,427,000 reports in the 12 months up to September 2021 leading to the removal of more than 50,500 scams and 90,100 malicious URLs.



Exercise in a Box
A toolkit of realistic scenarios that helps organisations practise and refine their response to cyber security incidents in a safe and private environment. This year, the number of users (multiple per organisation) using Exercise in a Box has risen by 56% (from 7,535 to 11,754).

Logging Made Easy
An open-source project that helps organisations to install a basic logging capability on their IT estate enabling routine end-to-end monitoring of Windows systems. This year, there were 1,063 unique clones of the LME code from the LME GitHub page for people to install it.

MyNCSC

The NCSC's tools and services are designed to improve an organisation's approach to cyber security. Although each service can be used in isolation, the best outcomes are achieved when these services are applied as part of a holistic approach.

In February the NCSC launched MyNCSC, a new platform as a single point of entry to its key digital services including Active Cyber Defence. MyNCSC brought together in one place access to tailored advice, services and alerts.

The new platform, which is due to replace the existing ACD hub, helps users reduce duplication, save time and better understand their security posture across a range of services. MyNCSC users are presented with service data, incident information and guidance to help them be more proactive in improving the security of their organisation.

At the time of publication, the platform was open to eligible users as part of the pilot.

Suspicious Email and Website Reporting Services

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

The service, which was launched in partnership with the City of London Police, received more than 7,250,000 reports leading to the removal of more than 59,900 scams and 112,000 malicious URLs – many of which the NCSC would not have seen.

The NCSC worked with Microsoft to introduce an innovation to simplify reporting suspicious emails. Technicians created the Report Phishing tool for Microsoft Office 365 which allows reports to be sent directly to SERS, as well as their organisation's IT team, with one click of an on-screen button. To support this new tool the NCSC published guidance on how to install the button - which can be downloaded to an organisation's systems from Microsoft's AppSource site.

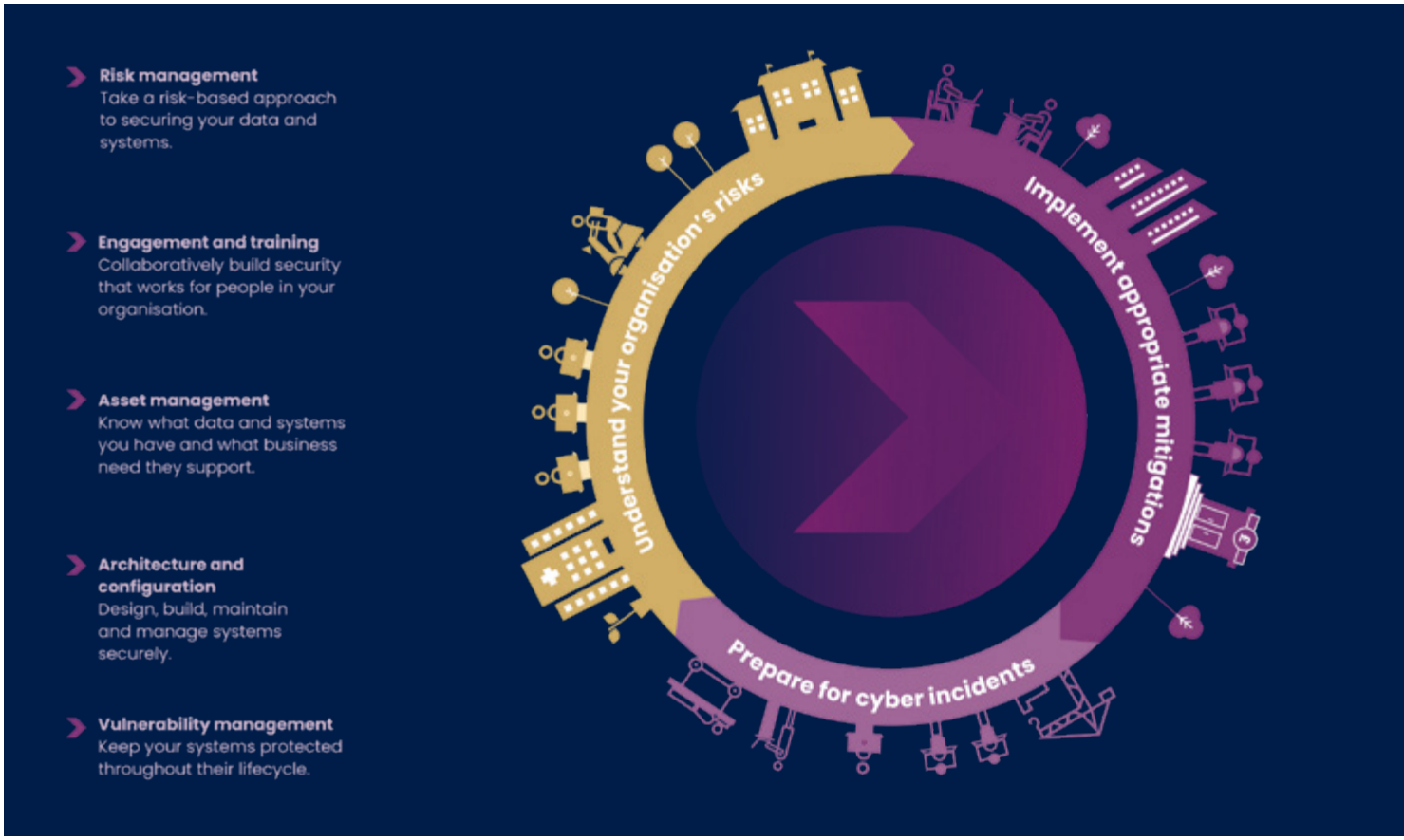
Building on the success of SERS, a new service was launched this year to enable the public to report scam websites. The Suspicious Website Reporting Service allows the public to report malicious websites for direct assessment by the NCSC, who can take them down if necessary. The NCSC has previously highlighted the problem of scam websites using fake news pages where celebrities such as Sir Richard Branson appeared to be endorsing enticing investment schemes.

How to report suspicious email and websites

To report a suspicious email forward it to report@phishing.gov.uk or use the Report Phishing Tool if installed on users' MS Office 365.

To report a suspicious website, visit ncsc.gov.uk/section/about-this-website/report-scam-website and follow the instructions

NCSC will assess the information provided and take action to remove the URL or scam.



10 Steps to Cyber Resilience

One of the NCSC's most popular pieces of guidance, 10 Steps to Cyber Security, was refreshed this year to reflect the changes in the way organisations and employees worked due to Covid-19, and the related cyber risks this posed.

Since the original advice was issued nearly ten years ago, there has been a growth of cloud services, the shift to home and hybrid working, and changes in the threats, such as the rise of ransomware and supply chain vulnerabilities.

This updated guidance aimed to help organisations manage their cyber security risks by breaking down protection into ten components. The guidance, which saw over 45,000 unique page views and 5,100 downloads this year, continues to be targeted at security professionals, and provides a route into more detailed guidance on specific topics.

"When it comes to defending against online threats, having relevant, timely alerts you can trust about malicious activity is vital for any organisation. The Early Warning service delivers on this, by providing organisations with specialised alerts and potential cyber threats affecting their networks. This will help them resolve security issues quickly and reduce the risk of serious harm being done."

Eleanor Fairford,
NCSC's Deputy Director for Incident Management

"I heard from a senior industry contact that a great many people look at our website as being the perfect version of giving information on what you should do in order to be secure as possible."

Paul Maddinson,
NCSC's Director for National Resilience & Strategy

Early Warning

One of the highlights of CYBERUK was the launch of the latest ACD service: Early Warning. This new free service was designed to help organisations defend against cyber attacks by circulating notifications about incidents and security issues.

Early Warning automatically filters intelligence from trusted sources to offer specialised warnings for organisations so they can take the necessary steps to improve their cyber resilience.

Subscribers to the service are granted benefits, including access to information feeds that are unavailable elsewhere. They receive tailored alerts, covering possible network compromises; notification of how their assets have been associated with undesirable activity or about their networks running vulnerable services that may need updating. Since its launch in May 3,924 organisations have signed up.

NCSC's response to Covid-19

In the Autumn of 2020, a range of UK academic and research institutions, critical to the strategic response to and recovery from the pandemic, were targeted in ransomware attacks. This included an attack on the University of Oxford while it was working on vaccine research crucial to the rollout of the national immunisation programme.

However, five months previously the NCSC had worked with universities, health and scientific institutions to review and improve their cyber resilience and implement services to prevent successful attacks getting through or mitigating their impact. This engagement was built on the shared experiences from the WannaCry ransomware attack in 2017.

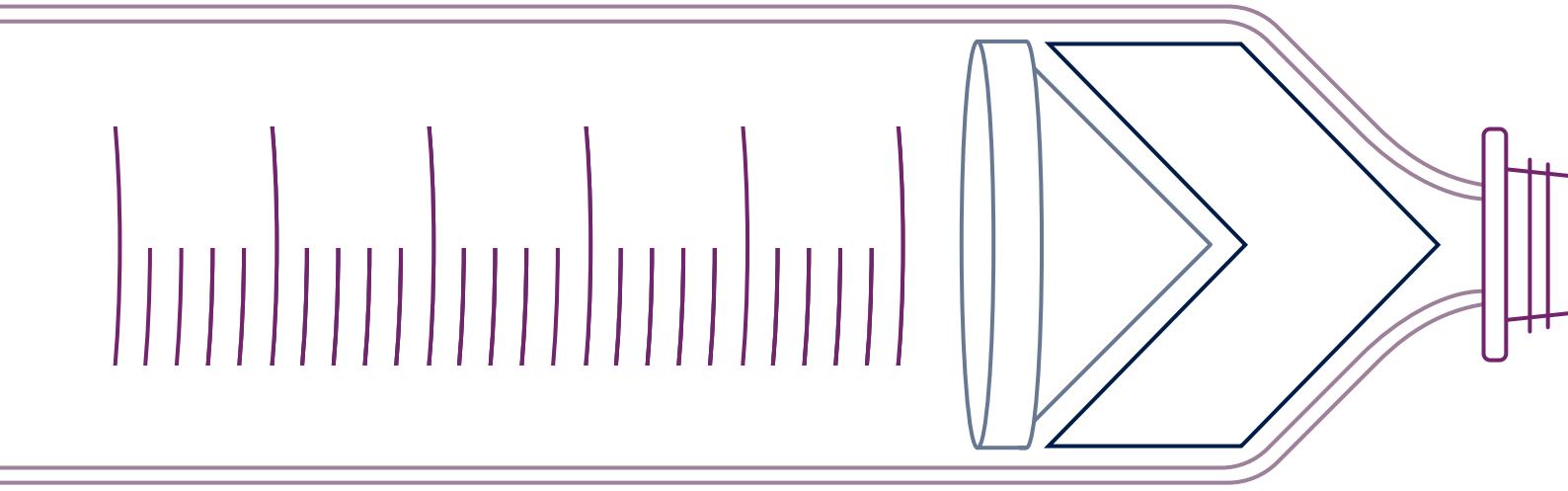
Since the outbreak, tens of thousands of indicators of compromise were shared to enable mitigating action by IT leads across the health sector.

The NCSC issued guidance and threat assessments to over 80 companies and 14 universities, and promoted its services such as Early Warning, Web Check and Mail Check.

A key intervention was to expand the use of Protective Domain Name System (part of the Active Cyber Defence programme that limits malware delivery and communication) to NHS, healthcare and vaccine suppliers, helping to protect these critical sectors from attacks.

In 2020 we extended the service to over 1,000 additional organisations within the Health and Social Care sector via HSCN in addition to our support of vaccine development and supply chain organisations.

Extension of PDNS to these critical sectors represents protection of 2-3 million additional employees, from essential workers providing and supporting front line care to those working to develop and deliver vaccines to citizens across the country.



"I'm really proud of the way this organisation pivoted to protecting the health mission at a time when it, and vaccine research and supply, were under sustained attack from ransomware operators who were putting people's lives at risk. We didn't wilt under the pressure of helping, with others, to protect the country under the Covid-19 pandemic."

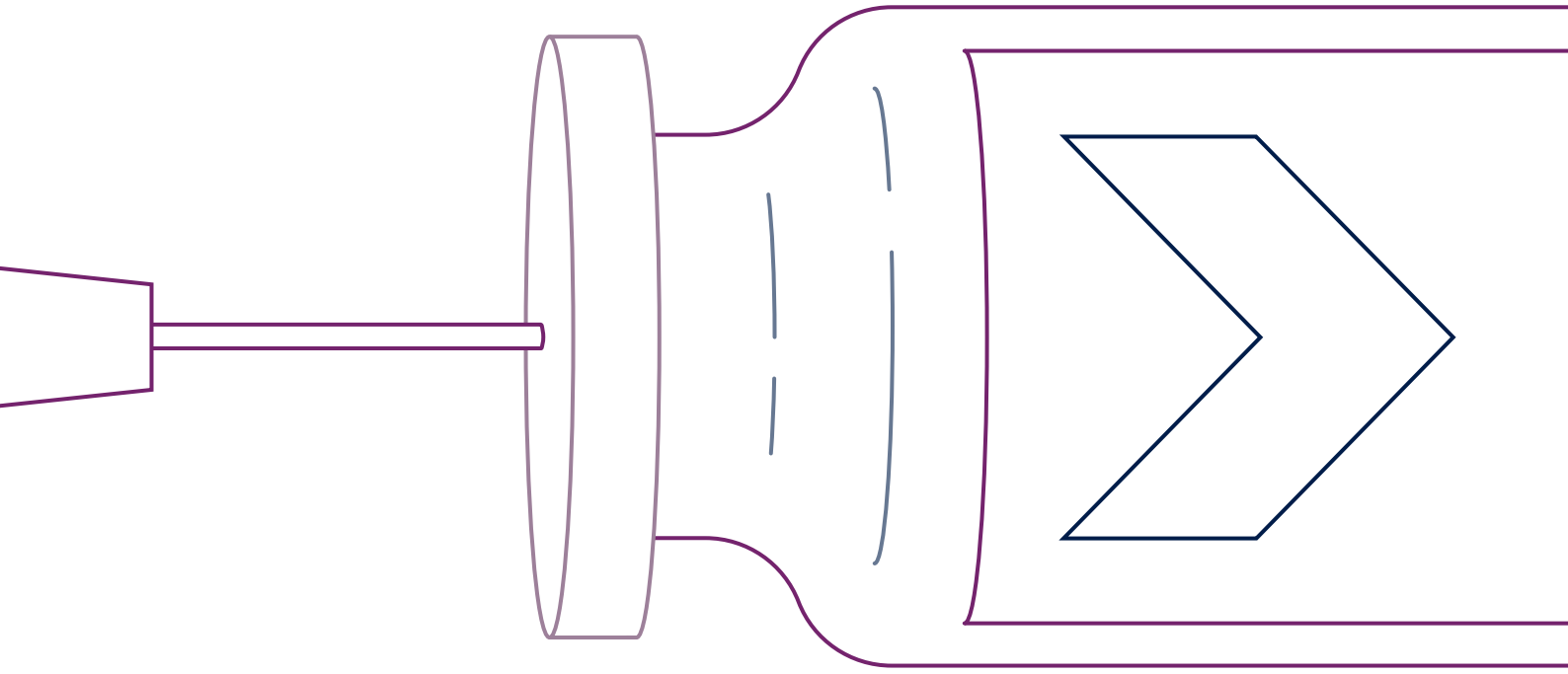
Dr Ian Levy,
NCSC's Technical Director

The NCSC also worked closely with NHS Digital to provide increased protection against cyber threats for health and care organisations during the pandemic.

The scope of the NCSC's work to protect the UK's response to Covid-19 went beyond traditional healthcare and supported sectors not previously seen as critical parts of the infrastructure, such as manufacturers of ventilators and PPE, care homes and supermarkets and their respective supply chains.

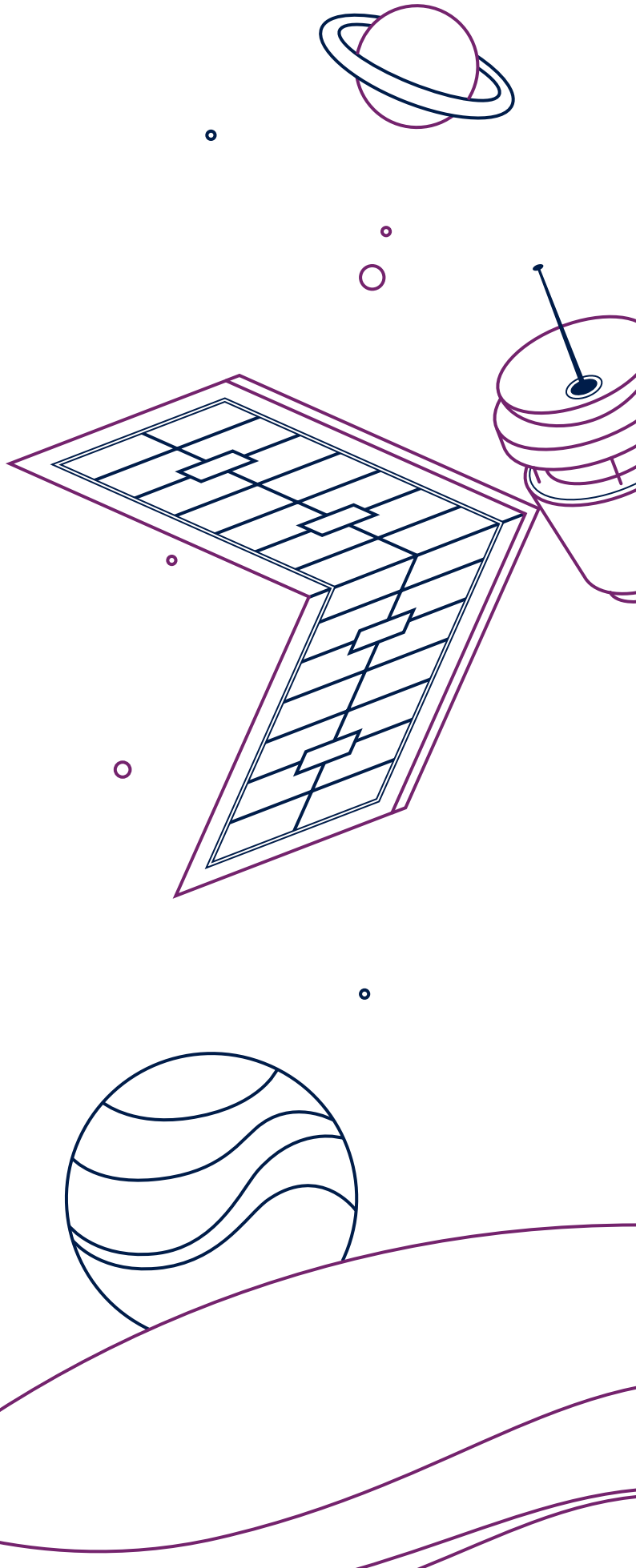
In total the NCSC engaged with approximately 5,000 organisations who were providing an essential service during the pandemic. These ranged from well-known brands through to small businesses vital to the response in supporting healthcare or to the public's ability to function during Covid-19.

The legacy for this work has seen hundreds of additional businesses now receiving support from NCSC and access to its services and tools, such as Exercise in a Box, Cyber Essentials and alerts.



Engaging and Supporting Sectors

From Critical National Infrastructure to communities, from the CEO to the citizen, NCSC has informed and engaged, and developed guidance and tools to meet those varying needs and priorities.



Critical National Infrastructure

Strengthening the resilience of the UK's CNI will always be a top priority for the NCSC, which is why it has continued to work with government departments, regulators, and private sector operators to ensure the latest threats, risks and vulnerabilities are understood and actions put in place to counter and mitigate them. The majority of this work is with sectors such as communications, finance, energy, water, transport and civil nuclear, but there is also work in several emerging sectors, notably Smart Cities, Smart Energy and Managed Service Providers.

This year the NCSC provided expert advice to the strategically important space sector – worth £16.4bn to the UK economy - to ensure future launch facilities were secure from outside interference and to improve the protection of those providing services, such as the decommissioning of old satellites and the removal of space debris from orbit.

The NCSC have collaborated with the UK Space Agency on industry training and government exercising and have taken a key role in the review of the National Security Risk Assessment where the NCSC's input on the threat to the space sector has ensured that the right risks are being prioritised.

As part of its ongoing engagement with the oil sector, the NCSC led a cross-organisation exercise on a ransomware attack affecting oil supply. This became a reality in the week preceding the exercise with the compromise of Colonial Pipeline in the US. NCSC worked with BEIS, industry and other government departments to help build a community of more than 50 of the largest organisations in the sector which is now collaborating on improving its collective cyber security.

This same collaboration made a real-world impact within transport, ports and the food supply chain, where the NCSC has worked to protect these key sectors as they contended with supply chains issues from the pandemic and changes to border controls, as well as their central role to vaccine supplies. This year a series of penetration tests were run at UK ports and the vulnerabilities found were used to advise on the steps needed to ensure better protection.

Financial sector

Working alongside the financial sector authorities, industry, law enforcement and trade bodies, the NCSC continued its efforts to improve the security and resilience of the UK's financial sector. The NCSC has provided support to the Financial Sector Cyber Collaboration Centre (FSCCC), an industry-led initiative which the NCSC helped to create two years ago.

The FSCCC exists to develop and share the latest understanding of threats to the sector. The FSCCC now consists of over 60 member organisations. This year FSCCC produced five threat awareness briefs, presenting the latest understanding of malicious activity against the sector. Four emergency calls have been held by the FSCCC this year, bringing potentially affected parts of the sector together to address imminent threats and serious vulnerabilities.

Armed Forces and National Security Assets

Working in collaboration with the Ministry of Defence, Armed Forces and defence industry partners, the NCSC continued to contribute to the protection of national security and defence assets this year.

The NCSC supported the development of the Digital Strategy for Defence, which set out plans for how the Armed Forces will use data to underpin technology; worked with the MOD on embedding secure-by-design principles and helped create a modern assurance and accreditation model. It established a team to maintain the highest levels of cyber security for the Continuous-At-Sea-Deterrent (CASD), including ongoing support to the Dreadnought Programme, which will replace the Vanguard-class submarine.

This year, the NCSC supported Carrier Strike Group 21 – the British-led naval force - as it began its first deployment to the Indo-Pacific. This included holding joint workshops with the Royal Navy and providing cyber threat intelligence and technical capabilities.

Image: HMS Queen Elizabeth

Case Study:

Devolved Administrations

The NCSC continued its partnership with counterparts and organisations in the Scottish, Northern Irish and Welsh governments. Particular focus was on supporting the response to Covid-19, providing:

- Technical advice to the Northern Ireland and Scotland contact-tracing apps, and, as Wales was using the NHS (England) app, advice on secure interconnectivity with NHS Wales's IT systems.
- Advice on the federated model to allow the various UK apps to communicate with each other.
- Advice on secure SMS and telephony for Covid-19 notifications to citizens – having notified on a potentially fraudulent SMS route, leading to a change to an assured routing.
- Technical advice to devolved vaccination booking systems, either where existing systems were repurposed or a new one created.
- Guidance and advice to businesses and organisations as they increased their online activity during the pandemic.

The NCSC supported victims of ransomware across the UK, including the attack against Scotland's environmental regulator in December. The Scottish Environment Protection Agency (SEPA) had more than 4,000 digital files stolen by hackers on Christmas Eve, and the NCSC supported SEPA in its response and recovery.

"As head of the Northern Ireland Cyber Security Centre my objective is to make Northern Ireland cyber safe, secure and resilient for its citizens and businesses. We provide support advice and guidance on cyber security and resilience matters at the local level, building out local networks and ecosystems that support this objective. Working with the NCSC gives us access to internationally renowned expert support, guidance and assistance that can be counted on. The NCSC provide support not only in their role as the UK's cyber technical authority, but also in helping develop and showcase cyber talent and skills development through initiatives like CyberFirst schools and CyberFirst competitions. These initiatives help Northern Ireland showcase its strength on a UK level encouraging cyber talent and leaders not only of today but also of tomorrow."

Joe Dolan, Head of the Northern Ireland Cyber Security Centre

"The Scottish Government has a strong, positive working relationship with the NCSC and we welcome the expert support and advice it provides to the people and organisations in Scotland. Their Scottish liaison officer, based in Scotland, provides good communication links in and out of the NCSC, ensuring early notification of cyber threats as well as details of new threat solutions are shared and used"

Clare El Azebbi, Head of Cyber Resilience Unit, Scottish Government

"The Welsh Government has utilised some of its National Cyber Security funding for a temporary outward loan post to the NCSC of two days per week. This has enabled more communication across Wales, promoting and increasing the use of the NCSC's advice, guidance and tools, particularly across the public sector. Some of the materials have been translated into Welsh, which again has increased take-up. The NCSC played a central role in exercising the Covid-19 vaccine roll out in Wales and is assisting the Welsh government in the technical aspects of the creation of 2 border check points."

The Welsh Government

Working with HM Government

The NCSC works in close partnership with the Government Security Group (GSG) and the Central Digital and Data Office (CDDO) in Cabinet Office to provide cyber resilience leadership across HM Government, including establishing the priority of cyber resilience and understanding of the threat at the highest levels of Government. We also work in close partnership with Cabinet Office to help HM Government and the Public Sector respond where incidents or significant vulnerabilities which have the potential to affect Government broadly. In particular the NCSC helped HM Government understand the SolarWinds and Microsoft Exchange attacks, providing mitigating advice and ensuring Government addressed vulnerabilities as soon as practically possible. Due to the government adopting ACD services the NCSC was immediately able to identify those departments who had compromised versions of SolarWinds, and similarly those using Microsoft Exchange servers. This enabled swift mitigation advice to be given to those affected.

The NCSC provided specialist advice and guidance to many UK government projects, programmes and events this year.

We provided support to the G7 Summit in mid-June, advising on cyber security measures and exercising to ensure it was ready for any cyber incidents that might occur, from large scale Denial of Service attacks to ransomware incidents. Following on from G7 the NCSC turned its attention to support to the cyber security of COP26, taking place in November. We have created new guidance to support the cyber security of high profile to support these and similar kinds of events.

As well as working directly with HM Government Departments, the NCSC has developed guidance which address key shared cyber security related challenges. As the Covid-19 pandemic went through its second wave, we issued further guidance on managing risks associated with a Bring Your Own Device strategy and Working from Home. The NCSC also played a key role in the evolution of the new Government Security Centres (GSECs) to increase the provision and broad availability of cyber security services across departments.

Local Government

This year saw increased uptake of core ACD services - Web Check, Mail Check, PDNS and Early Warning - among local government organisation and councils. For example, the use of PDNS increased from 72% to 80%[1] within local authorities.

With some local public services still affected months after cyber attacks taking place and recovery costs reaching millions of pounds (as confirmed by Hackney Borough Council) the NCSC continued to encourage more local authorities to take up these services to increase their cyber resilience.

Work continued on ensuring that cyber security formed part of incident response and civil contingency planning with local public services. The NCSC worked with the Ministry of Housing, Communities and Local Government[2] and the Welsh Government to support their ongoing work with local resilience forums to enhance cyber preparedness. This included encouraging the use of the updated Exercise in a Box package enabling users to practice their response to cyber security incidents.

Local authorities have increasingly adopted connected place (or 'smart city') technologies over the past year. The NCSC has published new Connected Places Cyber Security Principles to help ensure local authorities use these technologies in a secure and resilient way and is working with DCMS to provide advice and support to local government.

Supporting Small Business

At the start of 2020 there were 1.4 million small and medium-sized enterprises ('SMEs', 1-249 employees) in the UK employing 11.9 million people and turning over £1.95 trillion[3]. According to the DCMS Cyber Security Breaches Survey 2021, 38%[4] of SMEs surveyed experienced a cyber breach or attack in the previous 12 months, in some cases losing thousands of pounds in income or recovery costs.

With so much at stake, the NCSC continued to place supporting businesses and boosting their resilience as a high priority. It worked to create and promote the use of tools and services for small and medium-sized enterprises, and in May launched an e-learning package for small businesses and charities to help reduce the risk of cyber attacks.

The NCSC launched the Cyber Essentials Readiness tool for organisations to apply basic cyber security principles as part of a joint certification scheme with DCMS. Cyber Essentials is described in more detail in Chapter 4.

As part of the continued offer to protect and support start-ups the NCSC, in May, published new joint guidance (with the Centre for the Protection of National Infrastructure (CPNI)) to help fledging tech companies, and their innovations, keep secure. The 'Secure Innovation' guidance was developed in consultation with emerging technology companies and highlighted the importance of laying strong security foundations for startups, in a cost-effective and proportionate manner to protect their ideas, designs and intellectual property.

In October the NCSC revamped its Small Businesses Guide to help the sector operate more securely online. The new guidance arrived at a time when many organisations had moved their operations online due to the pandemic, and it highlighted accessible and affordable steps to take.

In October the NCSC supported the British Retail Consortium in its refreshed Cyber Resilience Toolkit for Retail. This contained an actionable guide designed for non-cyber experts, such as Board members, those in senior strategic roles, and startup businesses.

1 On 31/08/2020, 291 of 404 local authorities were using PDNS (72%). On 31/08/2021, 318 of 398 local authorities were using PDNS (80%). Note: on 01/04/2021 the number of local authorities decreased from 404 to 398

2 Later changed to Department for Levelling Up, Housing and Communities

3 According to the GOV.UK National Statistics Business population estimates for the UK and regions 2020

4 Calculated using a weighted mean

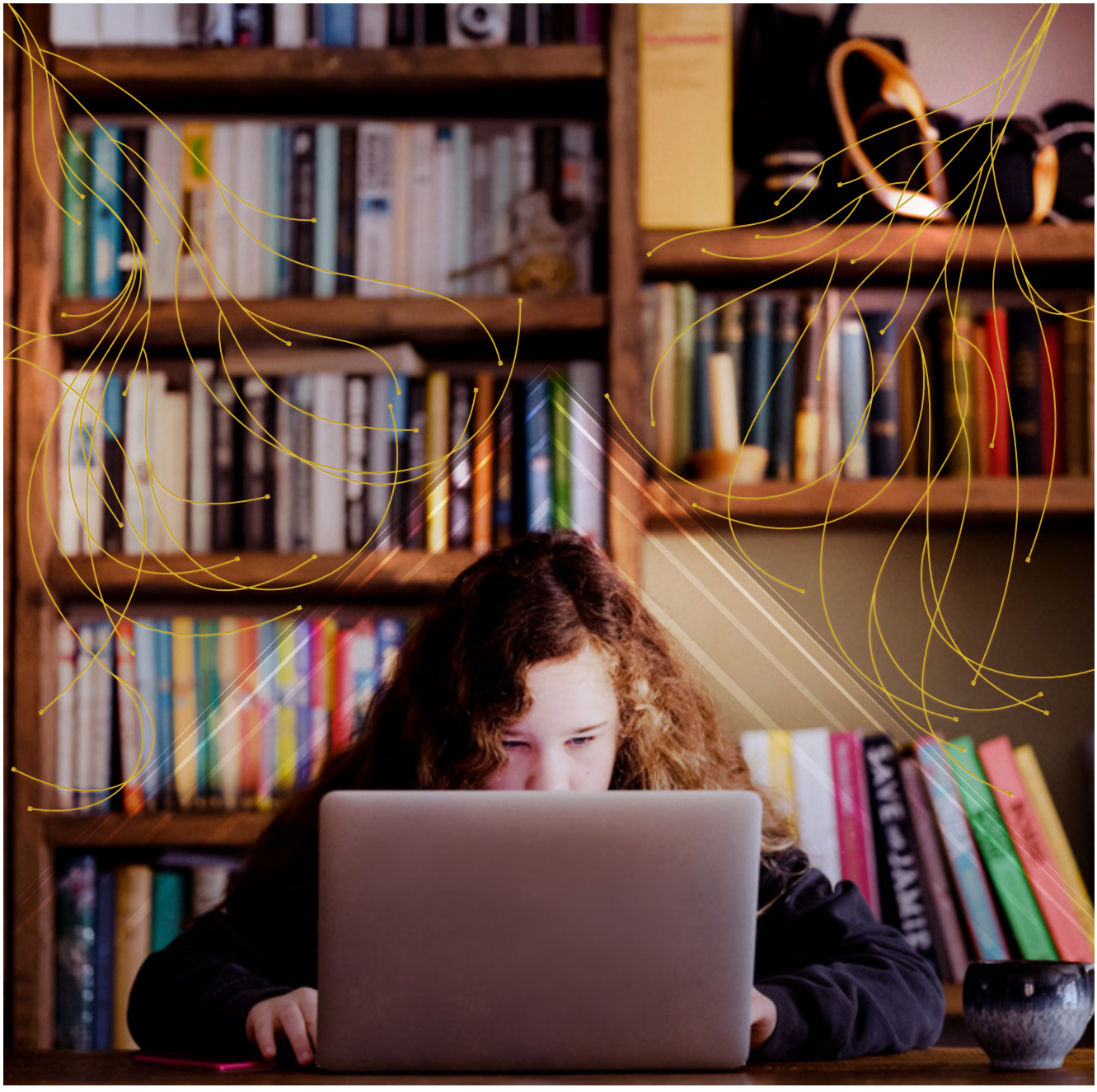
Education

Over the course of the 20/21 academic year there were persistent attacks against academia, leading to the NCSC issuing a cyber security alert direct to the sector in March.

The alert was published following a spate of online attacks against UK schools, colleges and universities from late February. Accompanying bespoke advice was created with input from the sector, while education leaders were encouraged to take swift action.

In April the NCSC launched a free online training resource for the education sector to improve cyber resilience in the face of the increasing threat and the resulting impact, with schools losing money, coursework and access to essential work systems for weeks.

A further alert was published as ransomware attacks against the sector escalated. It was recommended that schools take a 'defence in depth' strategy to prevent and mitigate attacks.



Engineering Processes

The NCSC identified that cyber risks can be introduced by security not always being fully considered in the engineering processes used to develop products used in critical national infrastructure (CNI). This is why, in October, the organisation teamed up with the Institution of Engineering and Technology to produce its first ever Code of Practice for Cyber Security and Safety in Engineering. The code of practice set out a series of principles designed to ensure safety and cyber security teams work together effectively to address the threat of cyber attacks.

Farming

In another first, the NCSC joined forces with the National Farmers' Union in December to issue a cyber security guide for the agricultural sector. With more farmers relying on and benefitting from digital systems and devices to monitor and manage their operations, it was important that these were kept secure from online threats.

Sport

In January the NCSC held its first security summit with professional sports clubs and organisations to help protect them against online threats. Over 180 representatives, including from 11 Premier League and 35 English Football League teams, rugby and cricket clubs and a range of national governing bodies, took part in coaching sessions with the NCSC's experts to better understand the threat and the actions to reduce the risk of falling victim to cyber criminals. The sports industry contributes £37 billion to the economy each year and was seen as a high-value target by cyber criminals, with at least 70% of clubs and bodies suffering a breach every 12 months - double the average for UK businesses.[5]

Construction and Manufacturing

The Department for Business, Energy and Industrial Strategy (BEIS) has been working closely with the NCSC to improve cyber resilience in two key sectors, manufacturing and construction. To raise understanding of cyber threats within the manufacturing sector, BEIS commissioned NCSC Assessment to produce a strategic threat paper on cyber threats to the manufacturing sector for release to industry, which was promoted in presentations at the Digital Manufacturing Week industry conference in November.
In the construction sector, NCSC have worked closely with CPNI and BEIS to support major construction companies in developing tailored information security best practice for companies engaged in joint ventures.

Early Years

Like most other work environments, nurseries and pre-schools became increasingly reliant on technology during the pandemic. As teachers and childminders often work with sensitive information, such as children's personal and medical data, the NCSC published its first-ever guidance for Early Years practitioners, giving advice on how to keep data and devices secure, and how to communicate with staff and families safely.

Supporting the citizen

Having cyber resilient citizens is a major part of the NCSC's mission to make the UK the safest place to live and work online. Improving cyber hygiene became even more of a priority as the pandemic took hold and more people spent time online to work, shop, socialise or communicate. The NCSC observed how cyber criminals were using the crisis to exploit new or inexperienced visitors to cyberspace and increased its engagement with the public.

As part of the Cyber Aware campaign the NCSC urged citizens and small businesses to follow practical behaviours, such as using three random words in passwords and using two-factor authentication, to ensure security online. In December it launched its first TV advertising campaign to inform citizens at a time of heightened risk as they went about Christmas shopping online.

In January the NCSC issued advice on how citizens could protect themselves from scams where their personal information had been compromised in data breaches, and it published cyber security guidance for new owners of recently acquired second-hand devices.

In February the NCSC launched a radio and digital campaign targeting at sole traders and micro-businesses, and the Cyber Action Plan: a new self-assessment tool to help users understand what steps they need to take to improve resilience. For the first time the NCSC advertised in ethnic radio stations and used small business influencers on Instagram to help reach a wider audience from diverse backgrounds.

The Cyber Action Plan was updated in May to accommodate citizens, creating a free, tailored action plan on the recommended steps to take to reduce the chance of becoming a victim of an online attack.

The campaigns saw increased uptake of the protective actions for both citizens and sole traders/micro-businesses: 16% of citizens and 8%[6] of sole traders/micro-businesses were reported to have started at least one of the protective behaviours since the marketing campaign relaunched in December 2020.

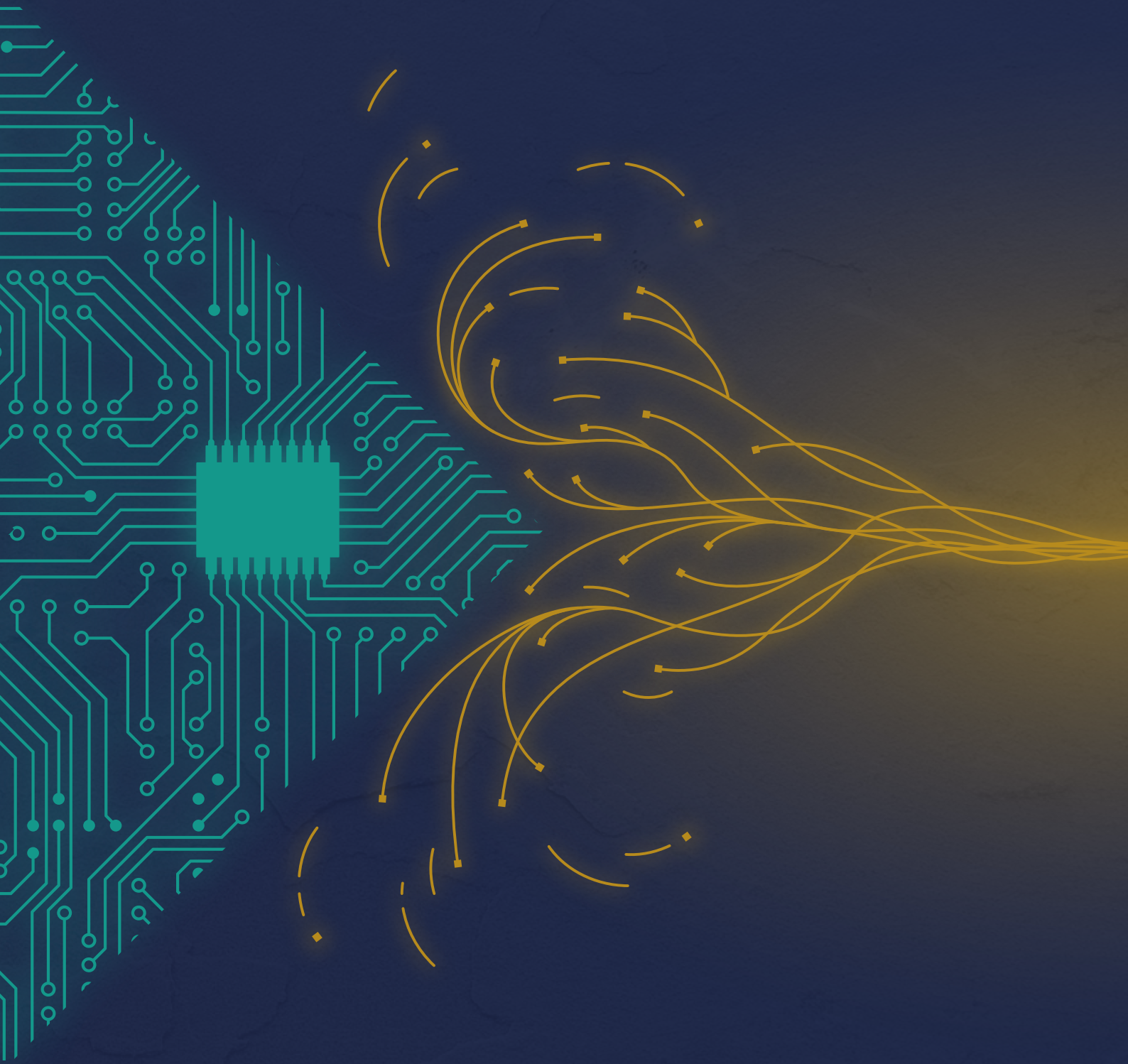
In partnership with the Department of Education, the NCSC launched an online cyber security game for children. CyberSprinters in which users race against the clock and tackle cyber security questions to score points and beat cyber villains, was aimed at 7 to 11 year-olds and came with a resource pack for primary schools and youth organisations.

5 According to NCSC report published 23rd July 2020 https://www.ncsc.gov.uk/report/the-cyber-threat-to-sports-organisations

6 Kantar Questionnaire, January 2021: "As a direct result of seeing or hearing these ads, did you do any of the following?", adults & sole traders/micro-businesses n=1500

Technology

How the NCSC is spearheading research and analysis to find new ways to secure the UK's digital systems



Technology

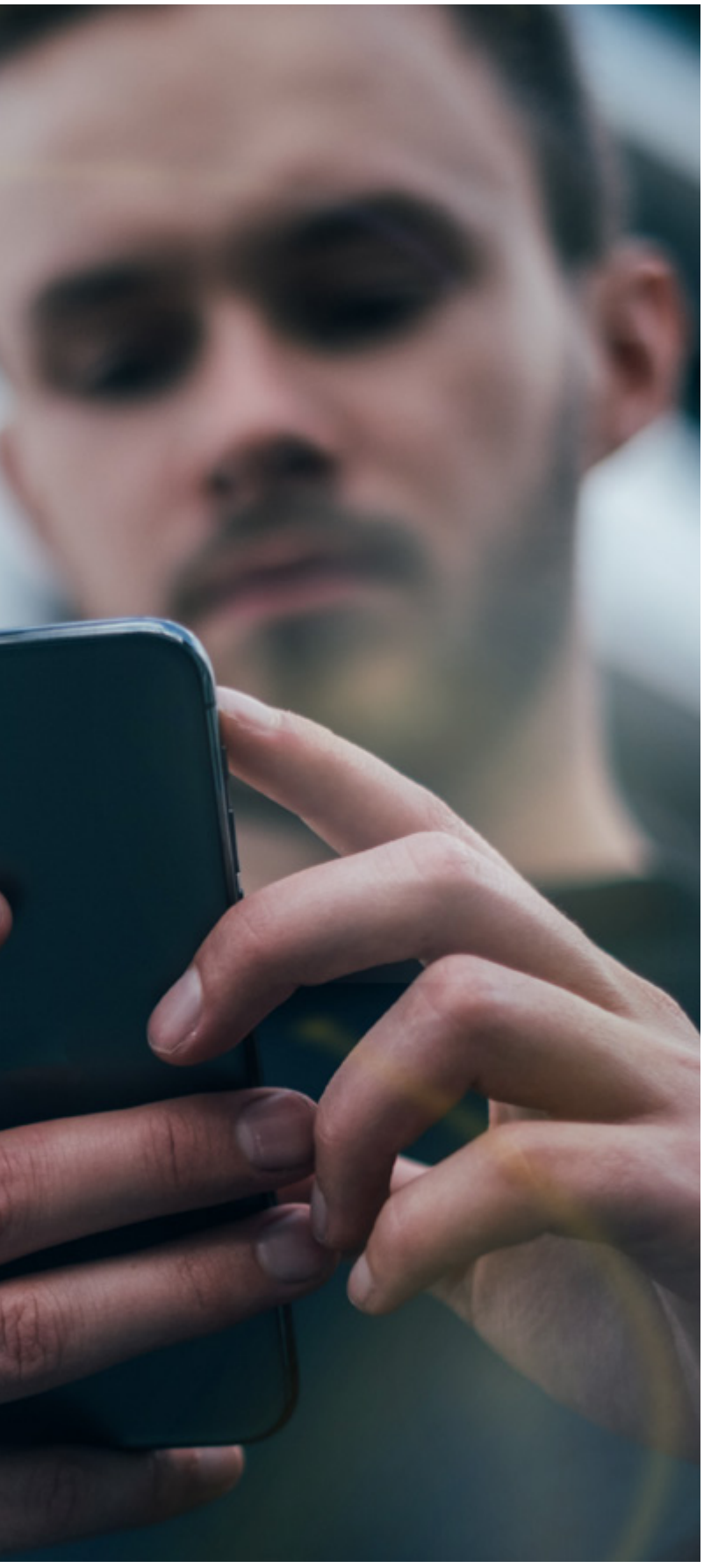
The aim of the NCSC's research programme is to manage long-term critical risks, and to strengthen the security of the critical systems that the UK relies upon. This includes defence and intelligence networks, national infrastructure, and the technologies used throughout our homes and schools.

The NCSC works with academia (sponsoring four research institutes) and industry partners (via the Initiate Portfolio) to share expertise across cutting-edge technologies such as artificial intelligence and quantum computing. Research isn't about quick wins, but it is vital to the UK's continued cyber security.

For national security reasons, much of the NCSC's research can't be described publicly. However, significant research achievements from the last 12 months are summarised below.

The Initiate Portfolio

Initiate is a cyber security research and innovation portfolio, run by the NCSC, that looks at future solutions for protecting government information. It's sponsored by the Ministry of Defence, Cabinet Office, the UK Intelligence Community and the Foreign, Commonwealth & Development Office, for the common good of them all.



‘Quantum-safe’ cryptography

Quantum computers use properties of quantum mechanics to compute in a fundamentally different way from today’s ‘classical’, computers. A quantum computer – theoretically – could break some types of cryptography currently used to protect classified systems. The NCSC has designed its first ‘quantum-safe’ cryptographic algorithms, designed to be resilient to such attacks. Next year the NCSC is aiming to get the quantum-safe version of our network cryptographic protocol PRIME ready for vendor use.

Digital contact tracing in the NHS Covid-19 app

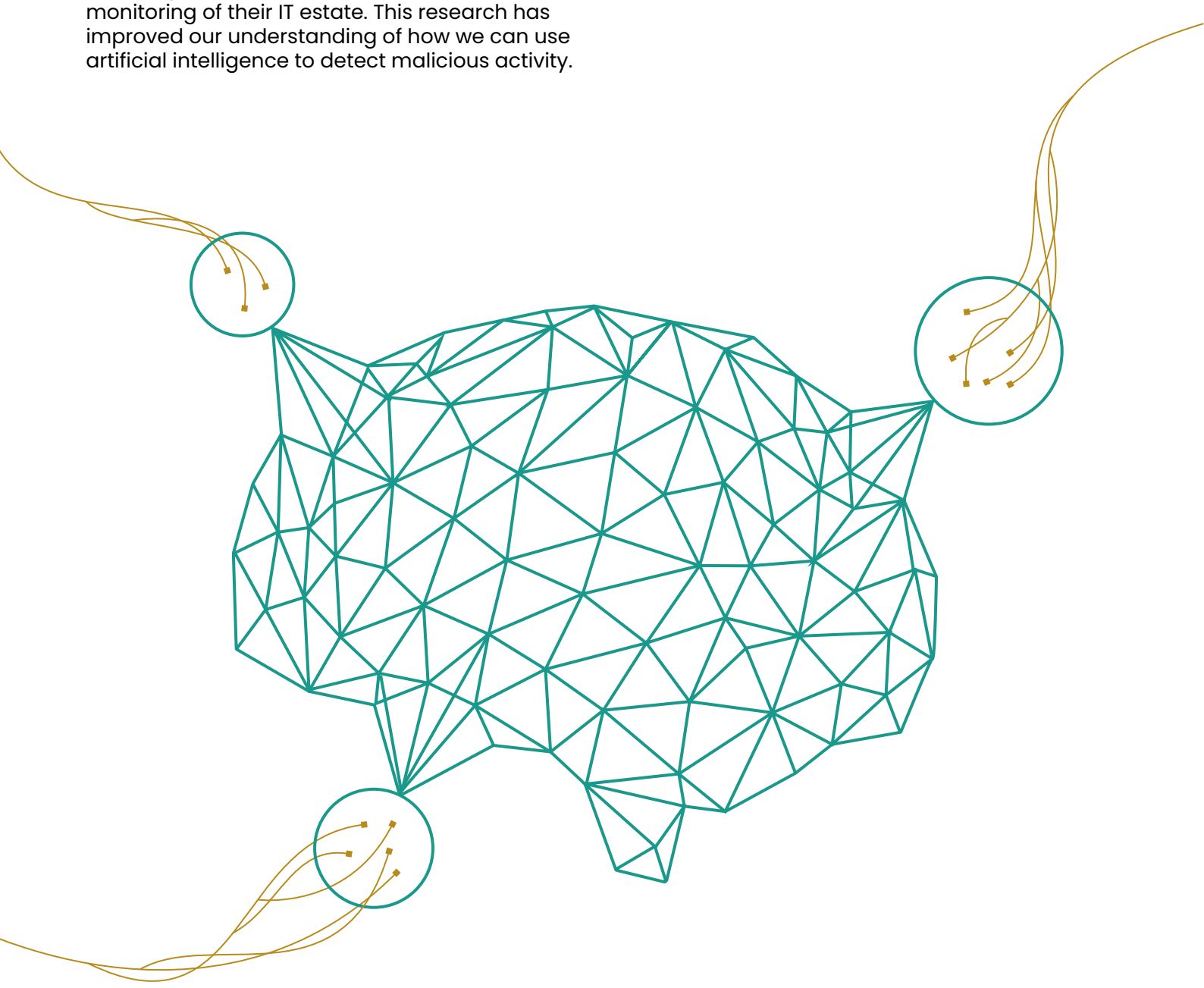
The NCSC’s radio frequency researchers, who typically work on military systems and communications, were deployed to help engineer the Bluetooth capabilities required by the NHS contract tracing Covid-19 app. Using Bluetooth to measure distance in the real world had never been done at this scale before. The NHS Covid-19 app has been downloaded 26.8m times in England and Wales, and became an important and trusted tool in the UK’s response to the pandemic.

Using artificial intelligence to detect malicious activity

The NCSC continues to work with the Alan Turing Institute (the national institute for data science and artificial intelligence) to explore whether machine learning can be used to detect certain types of cyber attack. The research built on the capabilities of 'Logging Made Easy', a tool developed by the NCSC that helps organisations set up a basic end-to-end monitoring of their IT estate. This research has improved our understanding of how we can use artificial intelligence to detect malicious activity.

Safeguarding the UK's critical systems

The technology used to protect the UK's critical ICT systems is usually bespoke, which makes the solutions on offer expensive to produce and limited in scope. The Shooting Star project was created to reach out to new small and medium enterprises (SMEs), and to make better use of commodity technology and standards.



Connected Places: new security principles for 'Smart Cities'

Following joint research with the CPNI and industry, the NCSC published a set of principles - believed to be the first in the world - outlining how to securely design, manage and build 'smart cities'. Smart cities use networked technology, such as Internet of Things (IoT) devices and sensors, to improve the efficiency of services for their inhabitants. This makes them potential targets for cyber attackers, due to the critical functions they provide and the sensitive data they process. The NCSC's 'Connected Places Cyber Security Principles' helps system owners, designers, vendors and operators to consider the high level security requirements that should govern smart cities.

To help bring the risks to life in a relevant way for the public, the NCSC's Technical Director Dr Ian Levy cited the 1960's film classic, The Italian Job, which featured one of the first Hollywood depictions of a cyber attack. For the launch Dr Levy said: "It was an attack against a city's centralised traffic management system. As part of an elaborate heist, a dodgy computer professor [played by Benny Hill] switches magnetic storage tapes for the Turin traffic control system to create a gridlock. Chaos ensues and the thieves escape with the gold.

"A similar 'gridlock' attack on a 21st-century city would have catastrophic impacts on the people who live and work there, and criminals wouldn't need physical access to the traffic control system to do it."

The NCSC has worked closely to support DCMS policy development on securing connected places, as well as promoting the security principles guidance to local authorities. This work includes NCSC playing a critical role in broadening awareness of the security risks among government departments and highlighting the broad scope of technology issues captured under the connected places umbrella.

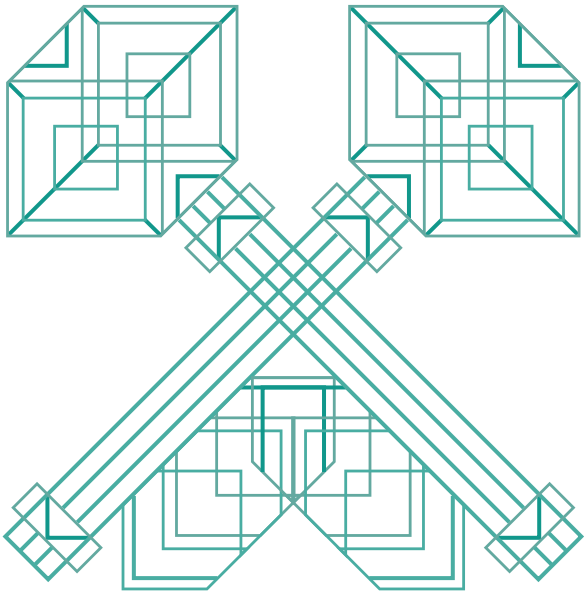
Verified high assurance software

Achieving the levels of trust and verification required for high assurance technologies has historically relied on hardware implementations. The NCSC funded a research study at the University of Surrey (the Faithful Composition of Trust [FaCT] project) which explored how verified software components can be used to create security properties previously only achievable through dedicated hardware support. This could be a game changer for reducing cost, speeding up time to market and achieving a reduction in size for physical products.

Research institutes

The NCSC supports four UK academic Research Institutes to develop cyber security capability in strategically important areas.

- The Research Institute for Sociotechnical Cyber Security (RISCS) is hosted by University College London
- The Research Institute in Verified Trustworthy Software Systems (VeTSS) is hosted by Imperial College London
- The Research Institute in Trustworthy Interconnected Cyber-physical Systems (RITICS) is hosted by Imperial College London
- The Research Institute in Secure Hardware and Embedded Systems is hosted by Queen's University Belfast



A new National Crypt-Key Centre

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 allies. In 2020, research on improving these systems led to significant new developments in Crypt-Key, transforming old, paper-based practices into modern, digital ones, to meet the advanced requirements of national and international partners. In November 2020, the NCSC launched a new NCKC, which will ensure organisations have access to more focused support to address their crypt-key challenges.

"Through the use of Crypt-Key we can ensure that the government is doing the right thing in protecting its sensitive operations and information, and we can make sure we manage the risk of interference from hostile states," said Andy W3, Deputy Director National Crypt Key Centre.

"We have the best people on the case to do this. We are world leaders in technology, and we have now got a cross-government grip on the capabilities we have wanted for a while, so we are in a good place."

Informing policy through technical advice and analysis

The NCSC provided technical advice to DCMS on the development of the Telecommunications (Security) Bill. The bill expands the legislative powers of the Communications Act (2003), and proposes new powers for the Secretary of State to remove from the UK's telecoms networks those suppliers identified as being high-risk.

The bill introduces a new security framework, constructed with the aid of NCSC analysis, which includes some 200 recommendations for operators to ensure the security and resilience of their networks. The NCSC also supported the DCMS in the creation of a Telecoms Diversification Strategy, which seeks to mitigate the risks of dependence on a limited number of equipment vendors for the UK telecoms sector.

The NCSC played an important role in the development of the National Security and Investment Act, which was introduced to the House of Commons in 2020, and is due to become law on 4 January 2022. The Act modernised the government's powers to investigate, and if necessary, intervene in mergers, acquisitions and other business deals that may otherwise damage the UK's national security. The Act covers 17 sensitive sectors of the UK economy, ranging from artificial intelligence to quantum computing to robotics, and investors may need to seek government approval for acquisitions in these sectors. Equally, the Act will allow for greater transparency about the types of deals that the government may need to investigate, as well as more efficient learning processes for those acquisitions.

Nicola Hudson, the NCSC's Director of Policy & Communications said: "The Act will give investors additional certainty and clarity in investments in sensitive economics sectors as the UK enshrines its status as a global champion of free trade and investment, as well as providing an effective tool for the UK government to protect our national security in a rapidly changing world."

The Home Secretary, Priti Patel, pledged an imminent Government review of the UK's 30-year-old Computer Misuse Act (CMA) in a speech at the NCSC's CYBERUK conference.

"As part of ensuring that we have the right tools and mechanisms to detect, disrupt and deter our adversaries, I believe now is the right time to undertake a formal review of the Computer Misuse Act," she said.

Originally passed in 1990, the CMA was last significantly amended in 2008 to extend its scope and increase the maximum sentences available for core offences.

"We are launching a call for information on the Act this year," said Ms Patel. "I urge you all to provide your open and honest views on ensuring that our legislation and powers continue to meet the challenges posed by threats to cyberspace."

Huawei Cyber Security Evaluation Centre

Drawing on extensive analysis from the NCSC, the Cabinet Office published the sixth Huawei Cyber Security Evaluation Centre oversight board report into Huawei's presence in the UK. The report provides detailed analysis of the company's software, engineering and cyber security processes, and details the actions required of the company as a result.

The NCSC's Research Problem Book

The NCSC Research Problem Book describes broad themes of its research work. The key areas of unclassified activity include:

- Cryptography fundamentals - their security now and 'post quantum'.
- "Zero Day" exploits - how vulnerable is the UK to them.
- Adversaries' capabilities - what tools and capabilities are available to our most highly resourced adversaries?
- Device attestation – more detailed and authenticated status information from a connected device. How can we collect and analyse this data to improve decision making?
- Supply chains – securing ongoing confidence in the integrity of the UK's critical supply chains.
- Usability - how can we enable systems and products to be useably secure?

CYBERUK

The NCSC's CYBERUK conference is the nation's annual flagship cyber security event, bringing together government, national security, industry and academia to deliver world class content, cementing the UK's position as a responsible and democratic cyber power.

Due to the pandemic, this year's event was delivered entirely virtually via a dedicated open access YouTube channel. This platform allowed speakers, delegates and consumers to engage with CYBERUK more flexibly, including from the pop-up studio at the NCSC's headquarters in central London where the event was broadcast, their own office location or direct from their homes here in the UK or across the globe.

The programme included 20 hours of content, which was made more accessible due to the event's open format, and it focussed on the theme of "Building a resilient and prosperous digital UK following Covid-19". Technology enabled high-profile speakers from across the world to come together for keynote speeches, panel discussions and fireside chats delivered either live or via pre-recorded sessions.

This year's line-up of speakers and panellists included Sudhakar Ramakrishna, CEO of SolarWinds who spoke candidly to the NCSC's Director of Operations about the compromise at Solarwinds and the subsequent knock-on effect and impact across the globe.

Another first was a link up to the US with a conversation with Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technology for the White House, Beth Sizeland, Deputy National Security Advisor and Lindy Cameron. Among a wide range of topics discussed they covered the impact of the ransomware attack on Colonial Pipeline and the need to bolster resilience on both sides of the Atlantic, and the ways to respond and recover from major attacks.

Representing the UK government the then First Secretary of State and Foreign Secretary, Dominic Raab, and Home Secretary Priti Patel delivered keynote speeches on major cyber challenges, such as the growing threat from ransomware and how the UK is taking a leading role in preserving a free and open cyberspace.

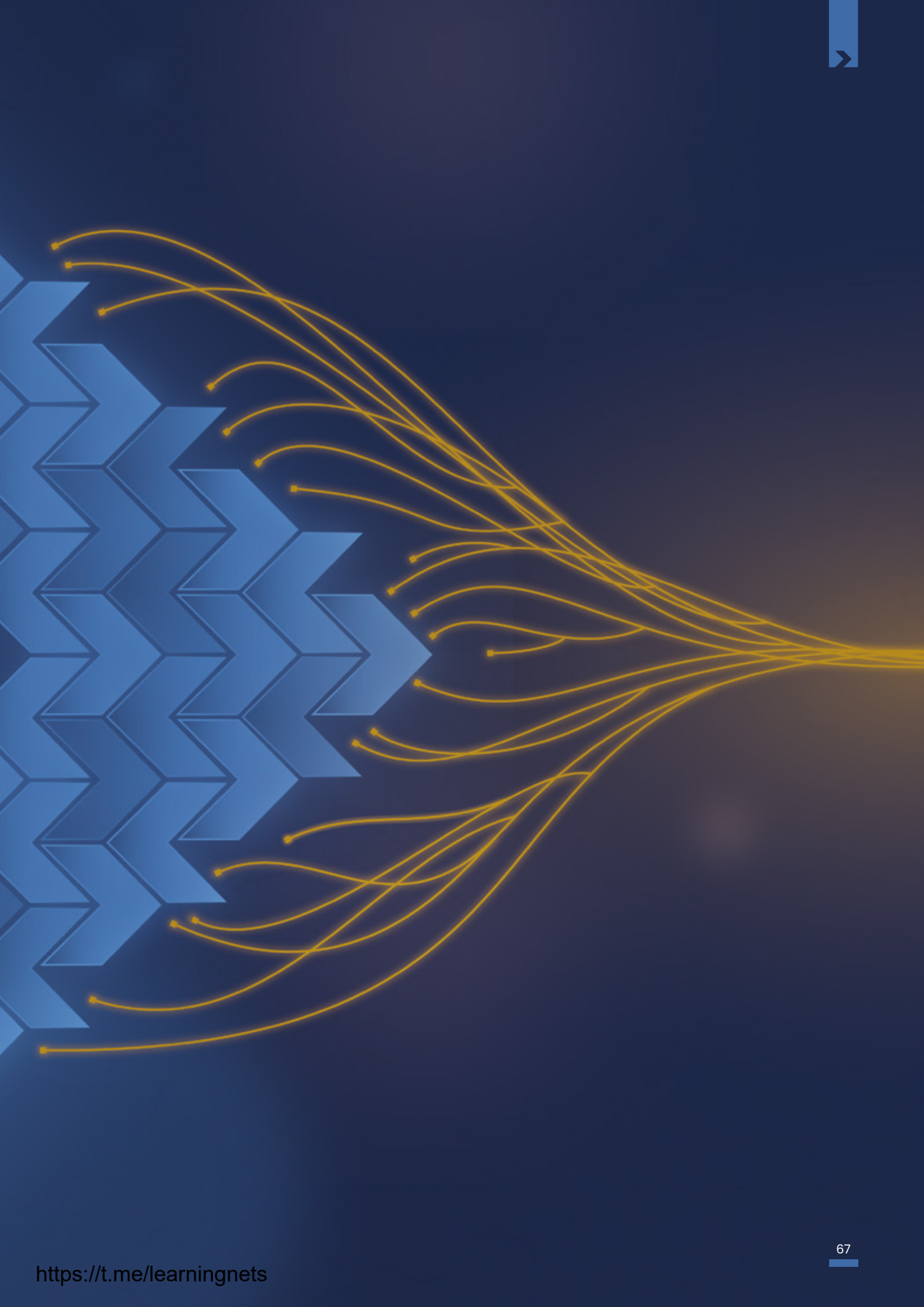
In addition to a series of live speeches and panels there were a number pre-recorded sessions where the NCSC came together with the government, academia and industry partners to explore the most important and relevant cyber security topics. Popular sessions included the development of secure connected places and smart cities, and ransomware in the education sector - the risk to schools and ways to prevent it.

Hosting the event on YouTube was a first for the UK Intelligence Community, reflecting the recent shift in the way the world lives and works. The technology brought CYBERUK to a global virtual stage, with viewers engaging across six continents and giving us our biggest audience yet: there were over 65,000 channel views in the first week of going live.

CYBERUK ONLINE 2021

Ecosystem

How the NCSC is strengthening and growing the UK's cyber security ecosystem



Ecosystem

While the NCSC works to confront and respond to threats, and bolsters the UK's resilience against them, the organisation has a key role in strengthening the country's thriving cyber security ecosystem. It is dedicated to helping the sector develop and grow into a skilled, innovative, diverse and confident force for good, able to defend and further the country's interests.

This chapter sets out how the NCSC is a central part of this system. From nurturing young talent, to creating further education opportunities, to supporting cyber startups, to testing and certifying standards in the security profession, to creating more diversity, to driving growth and innovation, to sharing best practice with the industry, the NCSC is making a positive, real-world impact to everyone's lives.

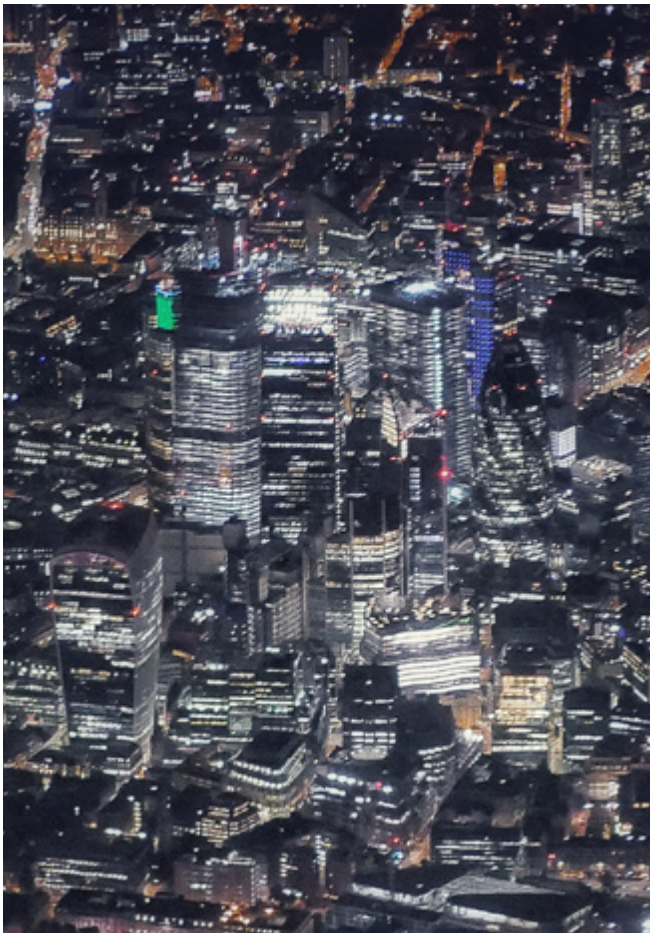
UK's cyber security sector at a glance

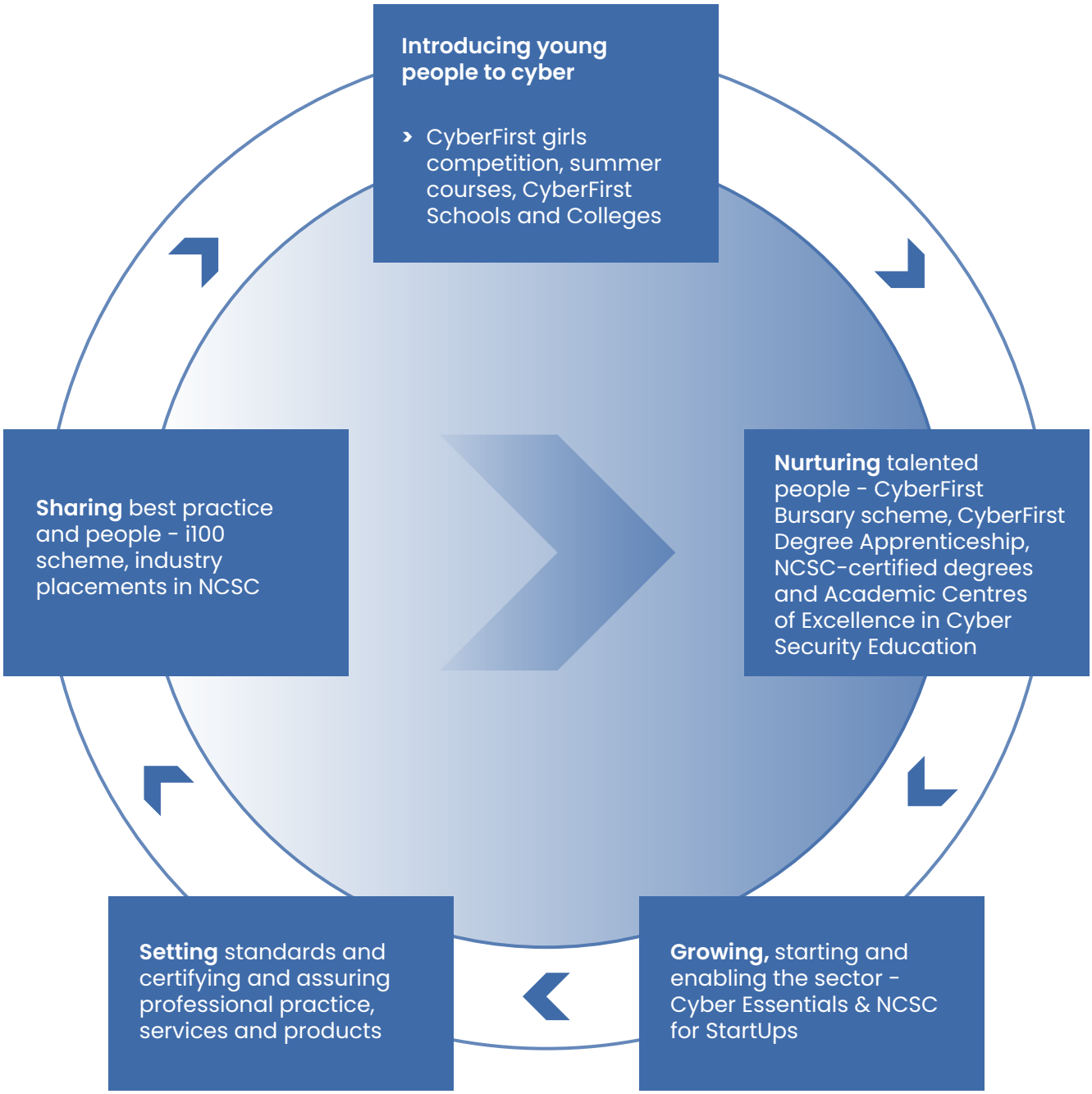
The UK has a strong and growing cyber security sector worth £8.9bn (up 7% on last year) with 1,483 companies (up 21%) and 46,683 people employed (up 9%). The UK is also the fourth largest security exporter in the world and cyberspace is an important and expanding part of that sector.

The unprecedented acceleration of digital transformation during the Covid-19 pandemic saw nearly £1billion of investment pumped into the UK's cyber security sector, with 4,000 new full-time jobs created.

"We are working with the UK's thriving cyber security industry to explore new ideas that will make the country the safest place to live and work online. The aim of our new initiative for startups, is to support those with pioneering ideas which in turn, encourages new skills, jobs and growth."

Chris Ensor,
NCSC's Deputy Director for Cyber Growth





Introducing young people to cyber

The NCSC continued to harness the best talent in the UK through several schemes, including CyberFirst. The programme, now in its fourth year, it has introduced over 56,000 10 to 17 year-olds to the world of tech and cyber security. It covers a broad range of activities, including a girls only competition, summer courses and placements, a university bursary and degree apprenticeship scheme, and its new CyberFirst Schools and Colleges initiative.

This year, more than 6,500 girls from 600 schools entered the **CyberFirst Girls Competition**, which was set up to help address gender diversity in the sector, and since its inception, 43,000 pupils have taken part. In April's final a team of year eight girls from Highgate School in London was crowned UK cyber security champions. NCSC CEO Lindy Cameron praised the team, called the Algorithm Alphas, for their innovation and skills in tackling the challenges of cryptography, logic and networking.

As part of the **CyberFirst Schools & Colleges scheme**, 27 schools and colleges were recognised by the NCSC for their commitment to cyber security education. The initiative is a collaboration with schools, businesses and organisations which aim to encourage young people into tech or computer science. Of the 27 schools, based across England, Wales and Northern Ireland, nine were given the gold award, 14 received silver status, and four got bronze. The institutions offer students a variety of engaging activities such as lunchtime coding clubs and sessions where pupils could pitch Internet of Things concepts. In February the NCSC announced it was extending the scheme to other regions in England.

This year, 1,736 pupils aged 14 to 17 took part in **Summer Courses** across 1,269 schools. The students, who could attend in person or virtually, got the chance to examine topics including digital forensics, ethical hacking and cryptography. The virtual element this year saw more teenagers taking place and more diversity within the intake, with record numbers of applications from girls (37%) and ethnic minorities (45%).

The **bursary scheme**, which offers undergraduates £4,000 per year financial assistance and paid cyber security training each summer to help kickstart their career, was offered to 183 students this year, including 23% who were from ethnic minority backgrounds. In total the scheme has benefitted 913 bursary students, with 92% of graduates now in cyber security roles. 350 of those took summer placements this year at organisations like BT and IBM.

Higher Education

Building on the NCSC's long-running Certified Degree initiative, 12 UK universities were recognised as Academic Centres of Excellence in Cyber Security Education (ACE-CSE) at either gold or silver level. The universities had already demonstrated their credentials in delivering excellent specialist cyber security education and were also able to show evidence of a broader commitment to improving cyber security awareness and education across their campuses and in their local communities, through a coherent and achievable strategy for development and collaboration.

The year saw an increase in the range and geographical spread of universities offering an NCSC-certified degree at either undergraduate or postgraduate level. The number of NCSC-certified degrees at both levels increased by 44% meaning that, at postgraduate level, more than a third of UK universities offering a master's degree in Cyber Security now offer at least one NCSC-certified course. An increasing number of universities offering a certified degree are located in under-represented geographical areas and are reaching increasingly diverse communities.

This year the NCSC certified two integrated Degree Apprenticeships schemes for the first time. Offering the opportunity to learn while working, the degree apprenticeships offer a choice for many students not wishing to pursue a degree by the traditional route. Edinburgh Napier University and the University of the West of England working in partnership with Gloucestershire College, became the first UK institutions to gain provisional certification for their courses.

The NCSC's own **Degree Level Apprenticeship scheme** is a three-year programme where apprentices – who receive a starting salary of £22k and gain a degree - are exposed to advanced technologies along with practical insights into the innovative ways the NCSC leads cyber security for the UK. This year there were 33 new apprentices in the 2020 cohort, while 56 graduated into roles within the NCSC and parent organisation.

CyBOK

The record number of successful applications for degree certification was partly attributed to the NCSC requiring all new applicants to use the Cyber Security Body of Knowledge (CyBOK) to map their curriculum content. Using the CyBOK has given applicants more flexibility to design their courses to meet employer and student needs, while giving assurance to the NCSC that the course content is appropriate and within the realms of cyber security. The expansion of the CyBOK to 21 Knowledge Areas, with the addition of 'Formal Methods for Security' and 'Applied Cryptography' has further broadened the definition of what is in scope in cyber security teaching.

Growing the talent

As well as nurturing talented young people into the cyber security sector, the NCSC continued to translate talent into jobs, opportunities and growth. Building on the success of the Cyber Accelerator programme, which supported 40 new tech companies in raising more than £100m investment over four years, a new flexible and open-ended approach was created to help entrepreneurs solve some of the UK's most important cyber challenges.

In June the successor programme to the Cyber Accelerator, NCSC For Startups was launched. The new initiative retained the Accelerator programme's core purpose of nurturing new enterprises, and now features continual onboarding of companies, ongoing support to 'scale ups', and increased collaboration with the tech sector and investors.

For the new programme, tech entrepreneurs are invited to engage with the NCSC's experts in developing, pivoting, and piloting products and tools to defend critical areas of the UK's economy and society. In August the first five startups were chosen with the companies offering solutions to issues such as cyber fraud and ransomware.

The companies selected were:

- **PORGiESOFT –** SME software accurately detecting fraudulent emails and messages with AI reading in between the lines
- **Exalens –** a virtual security analyst for digital manufacturing
- **Enclave –** Zero Trust Network Access (ZTNA) for servers, serverless and service mesh
- **Meterian –** SaaS security platform that builds a scalable and sustainable line of defence for apps that use open-source software
- **Rebellion Defence –** using AI to defend national security systems against threats like ransomware

National Cyber Security Centre *For Startups*

NCSC For Startups is jointly delivered by Plexal in partnership with Deloitte, CyNam, Hub8 and QA. It offers advancement for startups at all stages of maturity, from those developing a Minimum Viable Product (MVP), to companies with established solutions looking to expand into new markets.

Case Study:

NCSC for Startups

From his work on the dementia ward of a south London hospital, Dr Dexter Penn was only too aware of the everyday difficulties faced by his patients.

What he had not realised was the extent to which the vulnerable, often confused by the increased digitalisation of banking, were victims of scams. It is estimated that some five million older people in the UK fall victim to con tricks each year, collectively losing £1.2 billion.

For Dexter, the subject was brought home to his ward when a patient with Alzheimers was tricked out of the money she had saved for her place in a care home.

"She lost everything, and when her only relative came to visit and she burst into tears, I resolved to help," said Dexter, who set about finding out how many patients had been deprived of their money.

Following his research he formed a company, Kalgera, to devise a technological solution to protect the access to victims' financial accounts which scammers had been exploiting. He built an app which was able to analyse past and present financial behaviour to identify risks and trigger personalised alerts.

He applied to the NCSC's Cyber Accelerator (now Startups) programme to help develop the app. He said: "Being on the programme gave us the opportunity to work with banks to develop our technology and help identify those customers who were at risk of financial abuse."

"I'm very grateful for the time it allowed me to reimagine the commercial side of things, and for the support we received from experts who helped us improve the security of our products."

Case Study:

Secure Schools

When home schooling became the norm during the pandemic, it meant an increased risk for schools, which faced the same cyber security threats as other organisations, but with extra sensitivity of data relating to pupils, parents and staff.

Secure Schools, founded by Paul Alberry and Jill Foster, developed an online tool that helped schools address three critical areas of cyber security: securing technology, awareness training and assurance.

Shortly before the first lockdown, the firm was selected to join the Cyber Accelerator programme (now NCSC for Startups).

Said Paul: "The biggest thing we gained was the breadth of experience from the NCSC's experts, who helped us grow our idea into a scaleable business.

"Educational institutions continue to face a tough challenge in defending against cyber attacks, but we are proud to have helped schools develop their own security programmes and to have trained thousands of staff to recognise and deal with cyber threats."

Setting standards, certifying professional practice and assuring services and products

Defining what 'good' looks like

The NCSC uses its technical authority to endorse the quality of cyber security products and services. In doing so, it is creating a trusted marketplace, one that helps consumers improve their resilience and raises standards. From products such as Smart Meters, to professional services like Incident Response or Cyber Security Consultancy, the NCSC defines what 'good' looks like - whether this is at a national level or for small businesses that need to meet growing requirements.

Cyber Essentials

The NCSC's Cyber Essentials scheme continued to help develop and grow the ecosystem while at the same time bolstering the UK's resilience to cyber attacks. The government backed scheme helps organisations, whatever their size, guard against a whole range of the most common cyber threats. This not only reassures customers and organisations of a foundation level of protection against cyber attacks, but increasingly government contracts often now require this basic certification too.

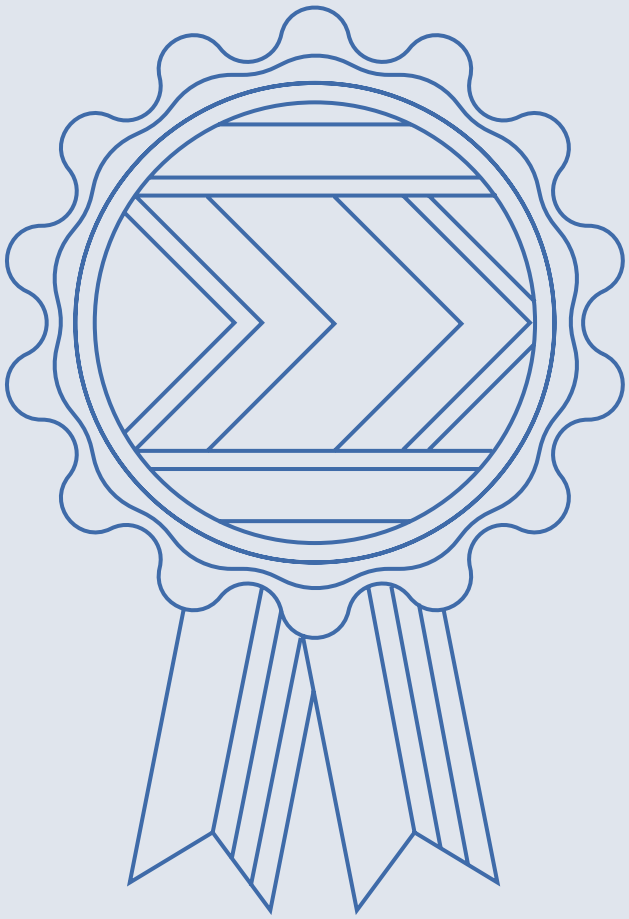
Since its launch, the certification scheme - which is jointly overseen by DCMS and delivered in partnership with The IASME Consortium - has awarded over 75,000 Cyber Essentials certificates to enable users to gain official recognition for understanding and applying a set of 5 basic technical controls.

In September 2020 NCSC helped DCMS deliver a £500,000 funding package to enable vital healthcare suppliers to improve cyber security and gain Cyber Essentials certification. The scheme helped 170 small and medium-sized businesses, including medical suppliers and primary care providers, improve their cyber resilience and ensure the continued delivery of services throughout the pandemic.

In May, to help organisations better understand what they need to do to attain this base level of security, the scheme developed further with the launch of the Cyber Essentials Readiness Tool. The free online resource, which was launched at CYBERUK, helps organisations prepare for the certification process by asking a series of questions about hardware, software, and boundary devices such as firewalls, as well as use of passwords. On completion of the survey, organisations are presented with a bespoke action plan that outlines the steps needed to prepare for the certification process. 11,181 users have used the Readiness tool since its launch with the biggest users being SMEs.

Through Cyber Essentials, the NCSC is fuelling the growth of the UK's cyber security industry, licensing the assessment process to certification bodies across the UK and Crown Dependencies. There are now over 273 cyber security companies licensed to deliver Cyber Essentials employing 803 assessors. Over 80% of these companies are micro and small businesses.

This year 24,806 Cyber Essentials certifications were awarded, including 4,591 organisations achieving Cyber Essentials Plus status.



CYBER ESSENTIALS

There are two levels of certification to demonstrate an organisation's implementation of a set of technical controls:

- Cyber Essentials, an independently verified self assessment
- Cyber Essentials Plus, has the addition of a technical audit by a qualified assessor

Benefits of being certified include:

- automatic cyber liability insurance for any UK organisation who certifies their whole organisation and have less than £20m annual turnover
- you can demonstrate compliance with government procurement rules
- reassure customers and potential new business leads that cyber security is taken seriously

Driving professionalisation in cyber security

As the cyber security sector continues to grow, and as more businesses and organisations consider their resilience or broaden their cyber security controls (for example to meet government procurement requirements) there has been an increasing demand for cyber security professionals and services.

To help identify varying levels of standards the NCSC updated its Certified Cyber Professional (CCP) scheme this year. This saw a move away from 'roles' to the certification of specialisms, allowing specialists to demonstrate their competence through rigorous assessment – setting a benchmark for cyber security.

In July the NCSC launched Risk Management as its first certifiable specialism under the revised scheme. A new 'Security Architecture' specialism is being piloted, with others expected to follow. The NCSC also announced it now formally recognised two levels of expertise in the cyber security professional as:

- **Certified Cyber Professional** means that the NCSC affirms an individual can apply their knowledge and skills in a range of organisations, with an ability to deal with technically more complex scenarios and different environments.
- **Associate Cyber Professional** means that the NCSC affirms an individual's expertise in a range of typical scenarios, and that they are an effective and skilled member of a team or within established organisational processes.

"As both an assessor and an applicant, and as someone involved in winning work and recruiting, CCP is the only scheme where the balance of academia, experience and human behaviours are assessed properly to ensure practitioners can operate independently. Applying such rigour provides a level of confidence in the people we trust to support customer needs, as well as the authority to act on behalf of the NCSC"

Ian Hughes,
Principal Security Consultant, Thales

Certified Cyber Professional assurance scheme

The NCSC developed the Certified Cyber Professional (CCP) assurance scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession.

The service sets the standard for UK cyber security professionals and is at the heart of efforts to build a community of recognised professionals.

Benefits of being in the scheme include:

- professional expertise and competence are independently assessed and verified by Certification Bodies (CBs) approved by the NCSC
- a growing community of recognised professionals whose specialisms stand apart from other practitioners
- Cyber Professionals can act as Head Consultants in an NCSC Certified Cyber Security Consultancy

UK Cyber Security Council

To support the government's wider work on improving cyber security skills and driving professionalisation, NCSC has also supported industry efforts to establish the new UK Cyber Security Council, funded through DCMS. This new organisation will be responsible for developing and embedding professional standards and career pathways across the wider cyber profession, and will look to build on the momentum of NCSC, government and wider industry work in this space to date.

Assuring Products and Services – increasing the NCSC's reach by harnessing the UK's Cyber Security Industry

As well as redefining what 'good' looks like for the cyber security profession, the NCSC has continued this year to set the standard for industry products and services. Through its Commercial Assurance schemes, the NCSC assessed industry offerings against these standards, and - if they were met – allowed these products and services to use the NCSC brand.

NCSC assesses and assures products and services across several areas:

- Security Verification Services: which includes CHECK, the penetration testing scheme run on behalf of the government.
- Certified Cyber Security Consultancy: including Risk Management, Security Architecture and Audit & Review – mirroring areas assessed by CCP specialisms
- Cyber Incident Response: to help companies respond to and recover from attacks, such as ransomware
- Product Assurance: all Smart Meters and recognised smart metering products in the UK must be assured by NCSC licensed labs

By creating a trusted marketplace that helps UK consumers improve their security, the NCSC continued to raise standards and assure the market. This work continued to support the UK economy by helping to open up opportunities to sell UK cyber security products and services to foreign markets.

Assurance

Key achievements this year

- **Certified Professional –** Launch of a new Risk Specialism. Now running a pilot for Security Architecture
- **Certified Training –** Mapping of Cyber security training modules to CyBoK means applicants can now decide between similar certified courses on the basis of the knowledge taught.
- **Incident Response –** Brokerage offering launched to help critical organisations get the right level of support quicker, with NCSC sharing knowledge with the supporting company for a more efficient approach. 10 victims have already been offered help.
- **Cyber Essentials –** 198 Covid-19 support packages were delivered to 170 health sector organisations. More than 50% said they will now continue investing in cyber security. Added benefit of supporting 21 small certification bodies through the pandemic.
- **Cyber Essentials Readiness Tool –** Launched at CYBERUK. In the last 12 months we have sponsored 1,689 pen tests and currently have 26 companies recognised under the scheme.
- **Certified Consultancy** now has 27 companies with 35 service offerings and 37 Head Consultants recognised under the scheme.

"Participating in the i100 programme challenged my way of thinking and allowed my firm to help the NCSC with their objectives in a really beneficial way. We all gained from the insight and relationships which developed through working together.

"It gave me the opportunity to collaborate with peers from the legal profession and to talk about the challenges we faced as an industry with more than a little sensitive data to manage. It also provided an open channel for the NCSC to provide feedback on events in the legal sector and ensured their guidance reached the desired audience."

The Information Security and Compliance Manager at a large European Law Firm and a member of the i100 Legal group.

Sharing best practice – and people

Having nurtured talent, supported startups, and set, certified and assured industry standards the NCSC has continued to welcome those from the sector it has helped to develop and grow through its Industry 100 (i100) scheme.

This initiative has continued to facilitate close collaboration between the public and private sector to challenge thinking, test innovative ideas and enable greater understanding on cyber security. Industry 100 secondees work across a wide range of short-term placements within the NCSC, normally on a part-time basis. This year contributors included representatives from the sectors of legal, finance, aerospace, telecoms, academia, oil and gas, nuclear and engineering.

Equality, Diversity and Inclusion

The NCSC continued its drive to improve the diversity of the cyber security sector. In addition to initiatives like the CyberFirst girls competition, the NCSC launched a second survey for those in the sector. The new assessment, conducted in partnership with the accounting firm KPMG UK was expanded to capture new benchmarks on disability, neurodiversity, location of workplace, employer size, and seniority.

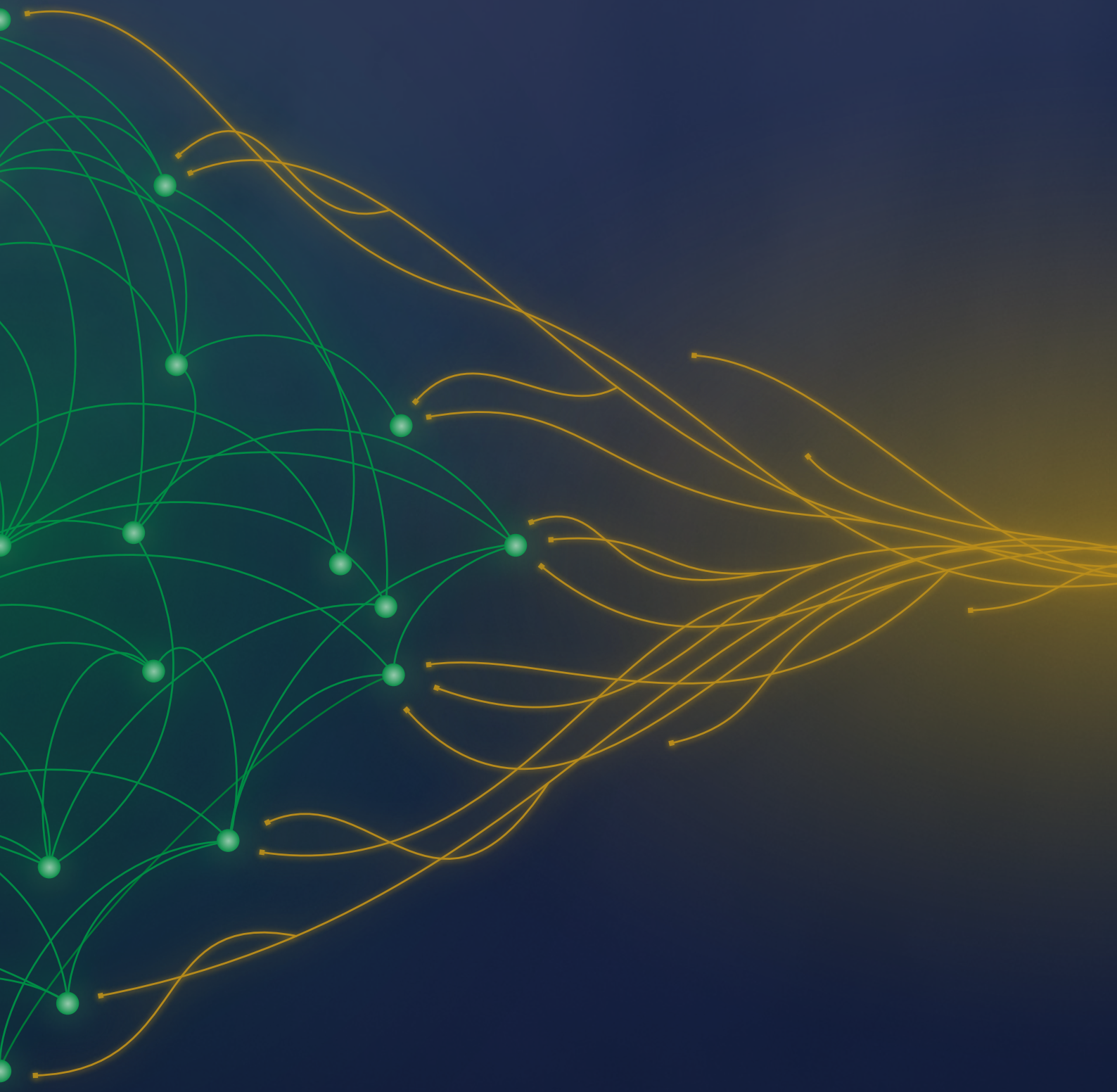
It will build on the results of the inaugural report which revealed that the sector does not benefit from the breadth of talent of the UK's rich and diverse communities, particularly with regards to a lack of inclusivity across gender, sexual orientation, social mobility, and ethnicity. It urged leaders to become accountable for diversity and inclusion within their organisations and for the industry to improve how it could learn from best practice within and outside the sector.

The NCSC accepted all of the recommendations from the first report and took a range of actions as a result, including the introduction of an Outreach Officer role designed to encourage people from under-represented communities to begin a career in the cyber security profession. The NCSC agreed that evidence suggested that a more welcoming community would lead to greater diversity, increased innovation, and better outcomes, which would help to provide greater security for the UK.

Data from the new survey will be used to identify areas needing further improvement as part of the NCSC's objective to transform the industry into an exemplar of best practice for diversity and inclusion, and to encourage a wide range of individuals to choose a career in cyber security.

Global Leadership

How the NCSC is advancing UK leadership in support of a free, open, peaceful and secure cyberspace



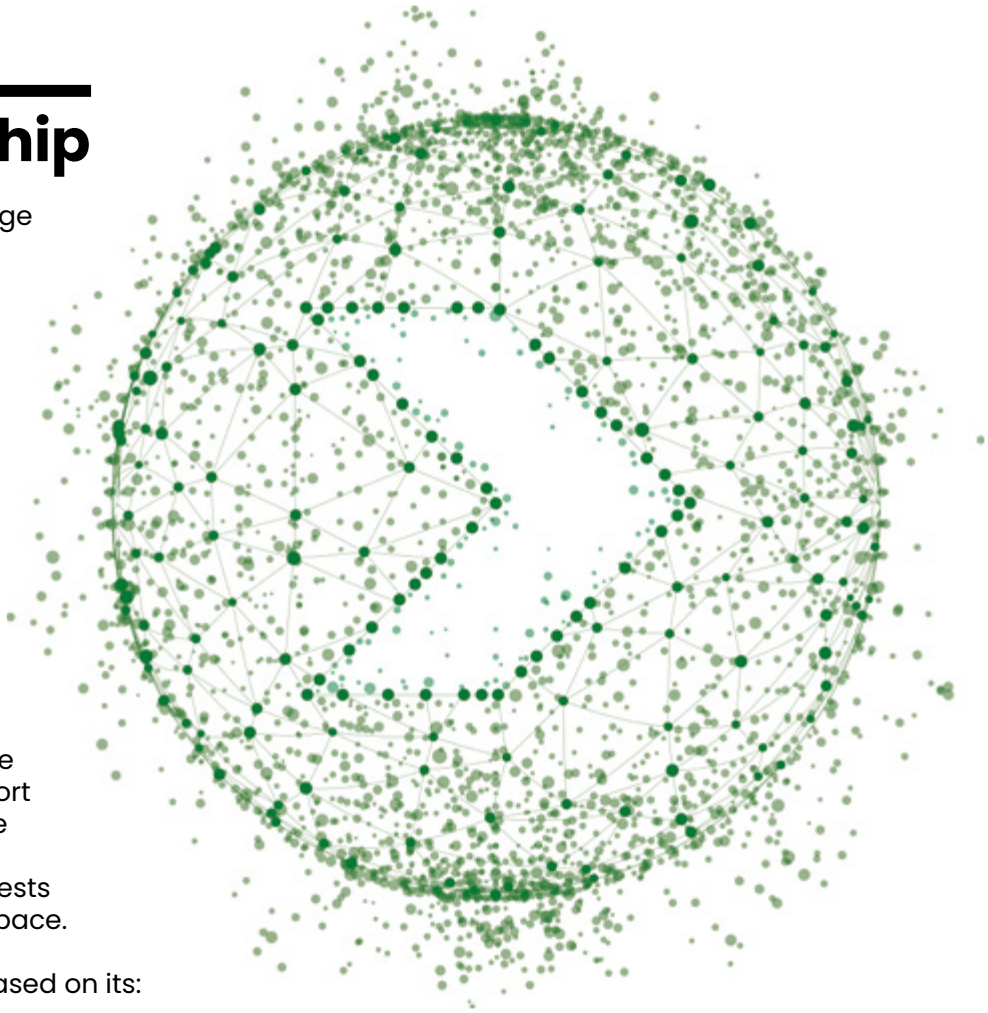
Global Leadership

Cyber security is a global challenge which demands an international response. Since its creation, the NCSC has worked closely with international partners and institutions to share information, capabilities and skills to help improve cyber defence. Although hampered by travel restrictions imposed by the pandemic, the NCSC continued to be a key player in the international effort to make the internet as safe as possible.

This section describes how the NCSC used its network of cyber security experts and leaders in the UK and around the world to support a free, open, peaceful, and secure cyberspace, and to protect and promote protecting the UK's interests as a responsible power in cyberspace.

The NCSC's global approach is based on its:

- **presence** (in multilateral organisations and standards development organisations, and ability to draw upon other government partners' overseas networks)
- **partnerships** (with other technical authorities, industry and academia)
- **capabilities** (unique ability to share intelligence with overseas partners, the NCSC's public-facing nature, and its robust strategic communications)



International Engagement for Real-World Impact

Over the past year the NCSC used its international partnerships to share the UK's understanding of current threats, exchanged intelligence, responded to cyber incidents, and developed its technical capabilities.

There was collaboration with international and industry partners to inform them of compromised credentials from a VPN vulnerability, which enabled them to inform victims and prevent and detect ransomware attacks.

As chair of an operational working group with the Five Eyes partners, the NCSC oversaw the first joint paper on common vulnerabilities published in July. It took a leading role in the first six-badged product between Five Eyes agencies (ACSC, CCCS, CERT.NZ, NCSC.NZ, NCSC-UK, CISA) on approaches to uncovering and remediating malicious activity.

A top priority of the NCSC's international agenda is to work with its partners to enhance their cyber resilience, by assisting in building their defence capabilities, and sharing best practice.

In April the NCSC, together with the UK Civil Aviation Authority (CAA), worked with the World Economic Forum (WEF) to shape international cyber resilience standards in the aviation sector. The NCSC's work shaped the eventual WEF report and provided another platform for the UK to advocate for its regulatory approach, specifically encouraging the use of the Cyber Assessment Framework as a regulatory tool to provide a common language and baseline of practice.

In May, the NCSC's Connected Places: Cyber Security Principles was widely welcomed, prompting its international counterparts to consider their own frameworks and how they could apply the same principles.

The NCSC and DCMS are actively working with international partners to learn as well as share best practice as we tackle the security risks which affect connected places.

The NCSC's mission of sharing its values with global partners to build a safe cyberspace was in evidence when CEO Lindy Cameron signed a Memorandum of Understanding with the Chief Executive of the Singapore Cyber Security Agency, David Koh, in November 2020. The agreement allowed the agency to use the NCSC's Exercise in a Box model to develop its own version. International travel restrictions meant the memorandum was signed by both CEOs via webcam.

Exercise in a Box is a key product in the NCSC's Active Cyber Defence toolbox. It allows organisations to practise their response to cyber security incidents in a safe and private environment, by providing realistic exercises and giving relevant guidance to ensure cyber resilience.

Case Study:

Vaccines International Engagement

The Covid-19 pandemic created new areas of vulnerability, in creating a new requirement to protect and secure vaccine and health sector supply chains. The NCSC engaged international partners on securing the overseas supply chains for vaccines critical to UK supply, and to enhance partners' resilience against the cyber threat to vaccines.

The NCSC liaised with manufacturers and other associated companies within overseas supply chains, assessing their cyber security, and offering protective advice. This included leveraging a network of international partners to work with 13 countries, as well as directly engaging companies and organisations (including the World Health Organisation, and GAVI, the Vaccine Alliance). It also shared threat information where possible, to raise awareness of the risks to supply chains, and worked closely with the UK's Vaccines Task Force.

This new area of collaboration provided immediate security benefits to the UK's vaccine and health sector supply chains and yielded longer-term benefits for bolstering the UK's international security.

Influence

The NCSC continued to further the UK's cyber security and interests around the world through providing expertise and analysis to define international technical standards; the norms and laws that govern cyberspace; and shaping partners' systems, models, and capabilities, to increase their cyber resilience.

In an area of vital importance to UK cyber security and future technologies, the NCSC initiated the creation of the first International Standards Group (ISG) focusing on Securing Artificial Intelligence. In the European Telecommunications Standards Institute (ETSI), which this year published GR SAI 002 on Data Supply Chain Security, the work on which this was based was led by NCSC. By collaborating with international partners, the NCSC was able to focus efforts on the vital topic of the provenance and integrity of data supply chains for Artificial Intelligence-based systems.

In an example of how the NCSC can deploy its technical expertise to shape UK international policy, the NCSC's cyber security expertise helped to inform and support UK negotiations led by the Foreign and Commonwealth Office, in the UN Government Group of Experts on State Behaviour in Cyberspace (GGE) and the UN Open Ended Working Group (OEWG), in which the UK played a leading role. Both groups agreed consensus reports amongst states; the GGE report included important text on attribution, and a landmark reference to international humanitarian law. The NCSC's expertise contributed to a compendium of national positions on how international law applies to state behaviour in cyberspace, which formed an annex to the GGE report.

The NCSC sponsored the UK-Gulf Women in Cyber Fellowship, which concluded its first cohort in 2021. Despite limitations in travel, work was completed with partners to sponsor the growth of a network of senior and up-and-coming women working in cyber security, in what is traditionally a male dominated profession and region. Amongst their successes, the Fellows conducted a survey and authored a report to identify regional skills shortages and provide national level recommendations and designed and built the first Arabic language cyber awareness resource portal in the Gulf, with advice aimed at making children safer online. The network is a powerful tool to build cyber resilience for key allies, highlight and promote senior women in cyber security, and promote UK values of equality and inclusivity in cyberspace.

And as more opportunities to travel opened, the NCSC's CEO was able to engage international counterparts in person, giving an opportunity to project thought leadership and presence overseas through speeches. In her address at Tel Aviv Cyber Week, Ms Cameron emphasised the importance of collective action to tackle global cyber challenges, including ransomware, supply chain security, global cyber governance, and a resurgent technological China.

"The NCSC's technical depth and expertise is simply outstanding. Our shared cryptologic history makes our close collaboration easy. I'm continuously impressed by how many outcomes are achieved by the NCSC in their cyber security mission, benefiting the UK and its allies."

Rob Joyce, Director for Cybersecurity at the U.S National Security Agency

Lindy Cameron addressing delegates at the annual Cyber Week hosted by Tel Aviv University

Similarly, in an address to the Institute of International and European Affairs, the CEO outlined the mutual threats faced by the UK and its international partners, and she reiterated the need for allies to continue to work towards a vision for the future, one of shared responsible behaviour in cyberspace.

"We are proud to call the NCSC a trusted partner and ally. No single entity can solve cyber security issues on their own and we value our close working relationship. We continue to work together to protect critical infrastructure sectors from cyber threats through regular exchanges. We also continue to share knowledge and threat information on important topics including cloud security, encryption, and cryptology."

The Canadian Centre for Cyber Security

Every section of this review is testament to the diligent and unceasing work of the NCSC's exceptional staff, whose achievements have made such an impression on me in my first year as CEO.

What you have read in the preceding pages simply cannot cover all the organisation's activities. As a colleague commented when I first asked about the scope of the review: "if it was to describe what each staff member contributes to the NCSC, the publication would probably be the size of the old Oxford English Dictionary" (which, for those interested in such data, ran to 15,490 pages).

Thanks to Covid-19, it has taken me longer to get to know the whole team than I would have liked, but what I have seen inspires me with pride and optimism, knowing that our organisation has a unique range of capabilities to tackle the most complex security issues. All of us are committed to keeping the internet as secure as we possibly can.

My heartfelt thanks to all in our organisation; for their hard work and dedication, especially in the extraordinary circumstances of a pandemic. We can all be proud of our collective teams' achievements, ensuring the online safety of millions of individuals and organisations, and we remain united in our mission to ensuring cyber security remains a top priority for the UK and around the world.

Lindy Cameron, CEO of the NCSC

ncsc.gov.uk/annual-review-2021

National Cyber Security Centre | Annual Review 2021

@NCSC

National Cyber Security Centre

@cyberhq

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

Designed and created by Agent Marketing Ltd. agentmarketing.co.uk