HM Government

# National Cyber Strategy 2022

## Pioneering a cyber future with the whole of the UK

# National Cyber Strategy 2022

## Pioneering a cyber future with the whole of the UK

# Contents

## Additional content

# Foreword

The United Kingdom is an open and democratic society, whose record in collaboration and innovation underpins our success as an outward-looking global nation. We see this in our response to international health emergencies and in our promotion of Net Zero targets. But nowhere are the advantages of this approach more evident than in cyber.

Whether it's realising the wide-ranging benefits that cyber offers our citizens and our economy as we level up and unite the entire country; working with partners towards a cyberspace that reflects our national values or using the full extent of our cyber capability to influence global events, the UK sees cyber as a way to protect and promote our interests in a landscape being reshaped by technology.

The new National Cyber Strategy is our plan to ensure that the UK remains confident, capable and resilient in this fast-moving digital world; and that we continue to adapt, innovate and invest in order to protect and promote our interests in cyberspace.

Taking over where the pioneering National Cyber Security Strategy of 2016 leaves off, this next chapter leads us into a future where the UK is even more resilient to cyber attack. As lead minister, I am clear about two of its core aims: first that we should strengthen our hand in technologies that are critical to cyber; second, that we should limit our reliance on individual suppliers or technologies which are developed under regimes that do not share our values.

UK science and technology will be the engine room of this change, ensuring that cyber continues to be a national economic and strategic asset, that our technology is more trustworthy and is better able to ward off a spectrum of cyber adversaries whose capabilities were, until recently, the sole preserve of nation states.

As a government, we have committed to spend £22 billion on research and development, and to put technology at the heart of our plans for national security. We have all seen the transformative potential of digital technologies but also, as with 5G, their potential to disrupt. Our plans for artificial intelligence and data policy will help ensure that we are on the front foot for these technologies, and the steps taken under the cyber strategy will ensure we have confidence in the security and resilience of suppliers and partners.

The creation of the National Cyber Force last year represents a significant step-up in our offensive cyber capability. But basic cyber security remains central to our efforts as we toughen up our response to those who attack the UK and our citizens. Our focus is also on making the public sector more resilient, helping councils protect their systems and citizens' personal data from ransomware and other cyber attacks.

As a society, cyber is for everyone. Through this Strategy, the government is doing more to protect UK citizens and companies, and its international partners – helping realise its vision of cyberspace as a reliable and resilient place for people and business to flourish.

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

# Introduction

## The opportunities and challenges of the digital age

**1.** Exponential advances in technology combined with decreasing costs have made the world more connected than ever before, driving extraordinary opportunity, innovation and progress. The coronavirus (COVID-19) pandemic has accelerated this trend, but we are likely still in the early stages of a long-term structural shift. The global expansion of cyberspace is changing the way we live, work and communicate, and transforming the critical systems we rely on in areas such as finance, energy, food distribution, healthcare and transport. In short, cyberspace is now integral to our future security and prosperity. This offers extraordinary opportunities for technologically advanced countries like the UK to pursue their national goals in new ways.

**2.** The scale and speed of this change – often outpacing our social norms, laws, and democratic institutions – is also unleashing unprecedented complexity, instability and risk. The past year has seen cyber attacks on hospitals and oil pipelines, schools and businesses, some brought to a standstill by ransomware, and commercial spyware used to target activists, journalists and politicians. The transnational nature of cyberspace means these challenges cannot be addressed without international collaboration, but it is also an increasingly important arena of systemic competition and the clash of competing interests, values and visions of our global future.

## Our vision: cyber power in support of national goals

**3.** In this context, cyber power is becoming an ever more vital lever of national power and a source of strategic advantage. **Cyber power is the ability to protect and promote national interests in and through cyberspace.** Countries that are best able to navigate the opportunities and challenges of the digital age will be more secure, more resilient and more prosperous in future. The UK is one of the world's most digitally advanced nations and this government has an ambitious technology agenda, at home and abroad. This means we are especially exposed to the challenges of cyberspace but also uniquely well-placed to lead the way in seizing its opportunities for our citizens and for the common benefit of humanity.

**4.** Over the next ten years, the internet, digital technology and the infrastructure that underpins it will become ever more fundamental to our interests and to those of our allies and adversaries. As we forge a new role for the UK in a more competitive age, strengthening our cyber power will enable us to lead the way for industry and other countries, get ahead of future changes in technology, mitigate threats and gain strategic advantage over our adversaries and competitors. It will make the UK one of the most secure and attractive digital economies to live, do business and invest in.

**5.** Our vision is that the **UK in 2030 will continue to be a leading responsible and democratic cyber power, able to protect and promote our interests in and through cyberspace in support of national goals**:

- a more secure and resilient nation, better prepared for evolving threats and risks and using our cyber capabilities to protect citizens against crime, fraud and state threats
- an innovative, prosperous digital economy, with opportunity more evenly spread across the country and our diverse population
- a Science and Tech Superpower, securely harnessing transformative technologies in support of a greener, healthier society
- a more influential and valued partner on the global stage, shaping the future frontiers of an open and stable international order while maintaining our freedom of action in cyberspace

**6.** Over the past decade we have established the UK as a cyber power, building cutting-edge cyber security and operations capabilities and a leading cyber security sector. This strategy builds on the significant progress made through the National Cyber Security Strategy 2016-2021 and three important conclusions set out in the government's Integrated Review of Security, Defence, Development and Foreign Policy. First, that in the digital age, the UK's cyber power will be an ever more important lever for delivering our national goals. Second, that sustaining our cyber power requires a more comprehensive and integrated strategy, considering our full range of cyber objectives and capabilities. And third, that this must be a whole of society approach – that what happens in the boardroom or the classroom matters as much to our national cyber power as the actions of technical experts and government officials, and working in partnership will be essential to our success.


CHELTENHAM
Science
Festival
18.2 Cyber Skills

## The five pillars of our strategy

**7.** The Integrated Review set out five 'priority actions' for this strategy and we will use these as the pillars of our strategic framework, **guiding and organising the specific actions we will take and the outcomes we intend to achieve by 2025**:

- **Pillar 1: Strengthening the UK cyber ecosystem**, investing in our people and skills and deepening the partnership between government, academia and industry
- **Pillar 2: Building a resilient and prosperous digital UK**, reducing cyber risks so businesses can maximise the economic benefits of digital technology and citizens are more secure online and confident that their data is protected
- **Pillar 3: Taking the lead in the technologies vital to cyber power,** building our industrial capability and developing frameworks to secure future technologies
- **Pillar 4: Advancing UK global leadership and influence for a more secure, prosperous and open international order**, working with government and industry partners and sharing the expertise that underpins UK cyber power
- **Pillar 5: Detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace**, making more integrated, creative and routine use of the UK's full spectrum of levers

**8.** Part 1 of this document sets out the strategic context we are operating in, the goals of our strategy, and the strategic approach we will adopt over the coming decade. Part 2 sets out the specific actions we will take to deliver our goals to 2025, organised under these five pillars.

# Vision

**The UK in 2030 will continue to be a leading responsible and democratic cyber power, able to protect and promote our interests in and through cyberspace in support of national goals.**

## Pillars and objectives

### Pillar 1

**Strengthening the UK cyber ecosystem**

1. Strengthen the structures, partnerships and networks necessary to support a whole-of-society approach to cyber.
2. Enhance and expand the nation's cyber skills at every level, including through a world class and diverse cyber profession that inspires and equips future talent.
3. Foster the growth of a sustainable, innovative and internationally competitive cyber and information security sector, delivering quality products and services, which meet the needs of government and the wider economy.

### Pillar 2

**Building a resilient and prosperous digital UK**

1. Improve the understanding of cyber risk to drive more effective action on cyber security and resilience.
2. Prevent and resist cyber attacks more effectively by improving management of cyber risk within UK organisations, and providing greater protection to citizens.
3. Strengthen resilience at national and organisational level to prepare for, respond to and recover from cyber attacks.

### Pillar 3

**Taking the lead in the technologies vital to cyber power**

1. Improve our ability to anticipate, assess and act on the science and technology developments most vital to our cyber power.
2. Foster and sustain sovereign and allied advantage in the security of technologies critical to cyberspace.
2a. Preserve a robust and resilient national Crypt-Key enterprise which meets the needs of HMG customers, our partners and allies, and has appropriately mitigated our most significant risks including the threat from our most capable of adversaries
3. Secure the next generation of connected technologies and infrastructure, mitigating the cyber security risks of dependence on global markets and ensuring UK users have access to trustworthy and diverse supply.
4. Work with the multistakeholder community to shape the development of of global digital technical standards in the priority areas that matter most for upholding our democratic values, ensuring our cyber security, and advancing UK strategic advantage through science and technology.

## Pillar 4

**Advancing UK global leadership and influence**

1. Strengthen the cyber security and resilience of international partners and increase collective action to disrupt and deter adversaries.
2. Shape global governance to promote a free, open, peaceful and secure cyberspace.
3. Leverage and export UK cyber capabilities and expertise to boost our strategic advantage and promote our broader foreign policy and prosperity interests.

## Pillar 5

**Detecting, disrupting and deterring adversaries**

1. Detect, investigate and share information on state, criminal and other malicious cyber actors and activities in order to protect the UK, its interests and its citizens.
2. Deter and disrupt state, criminal and other malicious cyber actors and activities against the UK, its interests, and its citizens.
3. Take action in and through cyberspace to support our national security and the prevention and detection of serious crime.

## Supporting national goals

- Security and resilience
- Science and Tech Superpower
- Economic prosperity
- Shaping the international order

# Part 1:
# Strategy

# Strategic Context

## Global Britain in a Competitive Age

**9.** The Integrated Review of Security, Defence, Development and Foreign Policy, published in March 2021, describes the government's vision for the UK's role in the world over the next decade and the action we will take to 2025. It recognises that for the UK to be better equipped for a more competitive world we must embrace innovation in science and technology to boost our national prosperity and strategic advantage. The National Cyber Strategy builds on this approach and its publication is one of the commitments under the Integrated Review strategic objective for 'sustaining strategic advantage through science and technology'.

## The cyber landscape

**10.** The policy challenges presented by cyberspace are not solely technological in nature. The cyber domain is a human-made environment and is fundamentally shaped by human behaviour. It amplifies such behaviours for better or worse, the impacts of which are usually also felt in the physical world. Cyberspace is owned and operated by private companies, governments, non-profit organisations, individual citizens and even criminals. This means that any strategic response to this context must link geostrategy and national security, criminal justice and civil regulation, economic and industrial policy and requires a deep understanding of the different cultural or social contexts and value systems interacting online.

**11.** Cyberspace also transcends national borders. Technology supply chains and critical dependencies are increasingly global, cyber criminals and state-based actors operate from around the world, powerful technology companies export products and set their standards, and the rules and norms governing cyberspace and the internet are decided in international fora. Cyberspace is also continually evolving as technology and the ways people use it change, requiring us to adopt an agile and responsive approach.

# Layers of Cyberspace

## What is cyberspace?

To many of us, cyberspace is the virtual world we experience when we go online to communicate, work and conduct everyday tasks. In technical terms, cyberspace is the interdependent network of information technology that includes the internet, telecommunications networks, computer systems and internet-connected devices. For the military, and when considering our efforts to counter threats in cyberspace, it is an operational domain, along with land, sea, air and space.

How is cyberspace experienced? Cyberspace is, by definition, a 'shared' space and its scale and complexity means that every person's experience of it is unique. Citizens access cyberspace when they check their bank accounts online or stream a film at home. Businesses use cyberspace to connect their staff with the resources they need, whether this is access to information or control over a manufacturing process. Governments provide public services to their citizens using online portals. Cyber professionals look 'under the hood' at the technology, standards and protocols that make it all 'just work' for users. All these groups use cyberspace in different ways and for different purposes, and we are all making an ever-greater use of it.

**Online experience**

- Email accounts
- Gaming profiles
- Social Media account
- Bank account login
- Contactless travel card ID
- Fitness tracker profile

**Software, systems and data**

- Enterprise IT systems
- Databases, e.g. HMRCs tax records
- Industrial control systems
- Windows/OS
- Apps, eg WhatsApp, Facebook, TikTok
- Programming languages, Python, C++

**Physical devices and communication**

- Routers, Hubs
- Servers
- WiFi, Ethernet
- Radio Antennas
- Smart fridges
- Contactless travel card reader
- Phones, PCs and other personal devices

## Cyberspace can be described in terms of three layers:

THE EXPERIENCE OF CYBERSPACE

### Virtual

The part of cyberspace most people experience. It consists of representations of people and organisations through a virtual identity in a shared virtual space. Virtual representations could be an email address, user identification, a social media account or an alias. One person or one organisation can have multiple identities online. Conversely, multiple people or organisations could also create just a single, shared identity.

### Logical

The part of cyberspace made up of code or data, such as operating systems, protocols, applications and other software. The logical layer cannot function without the physical layer and information flows through wired networks or the electromagnetic spectrum. The logical layer, along with the physical layer allow virtual identities to communicate and act.

### Physical

The physical layer of cyberspace includes all the hardware on which data is transmitted, from the routers, wires and hubs that you have in your home, to large complex telecommunications systems operated by big tech companies. As well as physical infrastructure it includes the electromagnetic spectrum on which data is transmitted, such as WiFi and radio.

## Cyber power

**12.** At the heart of our strategy is the concept of cyber power, which we define as the ability of a state to protect and promote its interests in and through cyberspace. We identify five broad dimensions of cyber power which align to the pillars of this strategy:

- The people, knowledge, skills, structures and partnerships that are the foundation of our cyber power, underpinning all the other components and integrating them into a national approach
- The ability to protect our assets through cyber security and resilience, in order to realise the full benefits that cyberspace offers to our citizens and economy
- The technical and industrial capabilities to maintain a stake in the evolution of key cyber technologies and deploy new advances in the interests of society
- The global influence, relationships and ethical standards to shape rules and norms in cyberspace in line with our values and interests and promote international security and stability
- The ability to take action in and through cyberspace to support national security, economic wellbeing and crime prevention. This includes cyber operations to deliver real world effect, and to help achieve strategic advantage, and law enforcement operations and the application of cyber sanctions to bring malicious cyber actors criminals to justice and disrupt their activities

**13.** Cyber power is distinct from more traditional forms of power. It involves seamlessly blending hard capabilities and softer levers of influence. It is more distributed and governments must work with partners in order to attain and exercise it. And the pace of technological change means that it can be gained and lost more quickly, as previously cutting edge capabilities are rendered obsolete by new advances.

**14.** Our strategy reflects this, describing how we will work with partners wherever we can as part of a whole-of-society effort. We will do more to address problems upstream and fix root causes, anticipate future trends and put in place long-term responses, and be more active in shaping rather than responding to the contested geopolitical environment.

## The UK as a cyber power today

**15.** The UK is already a leading cyber power.[1] Over the past decade the government has led a sustained national effort to strengthen the UK's cyber security, raise public awareness of cyber risks, grow the cyber security sector, and develop a wide range of capabilities through cyberspace to respond to threats from hostile actors. While we have made great progress and put ourselves in a strong position we still face significant challenges across the five pillars of this strategy.

[1] Ranked second in the International Telecommunication Union's Global Cyber Security Index, third in the Harvard Belfer Center's Cyber Power Index and in the second tier of the International Institute of Strategic Studies' Cyber Power capability assessment.

## The UK's cyber ecosystem and technology leadership

**16.** The UK's approach to building its cyber power has included concerted efforts to develop the country's cyber skills base and commercial capabilities, with the UK government and the devolved governments of Northern Ireland, Scotland and Wales working in partnership and learning from each other. The UK cyber security sector is growing fast, with over 1400 businesses generating revenues of £8.9 billion last year, supporting 46,700 skilled jobs, and attracting significant overseas investment. This sector is vital to our cyber power, supporting our security, and international influence and economic growth. We have consolidated the UK's reputation as a global leader in cyber security research, with 19 academic centres of excellence and 4 research institutes tackling our most pressing cyber security challenges.

**17.** The cyber security sector workforce has grown by around 50% in the last four years, with demand for skills often outstripping supply. We have engaged extensively with industry, professional organisations, students, employers, existing cyber security professionals and academia to better understand the nature of the cyber security skills challenge. We have made a wide range of extracurricular initiatives available to inspire young people to pursue a career in cyber security. From 2019 to 2020, we involved close to 57,000 young people in our CyberFirst and Cyber Discovery learning programmes. We extended our courses to reach younger students and the CyberFirst Girls' competition online attracted 11,900 girls, with the top teams competing simultaneously at 18 venues across the UK. Our CyberFirst bursary programme has attracted highly motivated, talented undergraduates. Last year there were 750 students in the scheme and all 56 graduates were in full-time cyber security roles.

**18.** Despite these interventions the wider skills pipeline still remains a significant challenge: of the 1.32 million businesses in the wider economy, around 50% still report a basic technical cyber security skills gap.[2] And although the UK cyber security sector has grown rapidly, most companies are startups and building large scale domestic vendors remains challenging in the face of international consolidation. As the experience with 5G has shown, the UK and our allies do not have a leading position in some key areas of the wider technology industry. Countries that are able to establish a leading role in the technologies critical to cyber power will be better positioned to influence the way they are designed and deployed, more able to protect their security and economic advantage, and quicker to exploit opportunities for breakthroughs in cyber capabilities.

## The UK's cyber resilience

**19.** Over the last decade we have delivered a wide range of interventions aimed at strengthening the UK's cyber resilience. This has been possible thanks to the significant and sustained investment in some of our core cyber capabilities, including the National Cyber Security Centre (NCSC), law enforcement and our security and policy professionals across government, as well as our expanding domestic and international partnerships.

[2] DCMS, Cyber security skills in the UK labour market 2021 (2021)

**20.** Our most innovative and groundbreaking efforts have been to take action at scale, including through the development and increasing roll-out of the Active Cyber Defence (ACD) programme. Last year it took down 2.3 million malicious campaigns – including 442 phishing campaigns using NHS branding and 80 illegitimate NHS apps hosted and available to download outside of official app stores.[3] We also took the lead globally in pushing for connectable consumer products to be 'secure by design', developing a UK code of practice in 2018 that inspired others to follow and informed the first globally-applicable industry standard on internet-connected consumer devices.[4] [5]

**21.** New regulation has had a positive impact on cyber security, with 82% of organisations saying the improvements they had made were influenced by the introduction of the UK General Data Protection Regulation in 2018.[6] And 77% of businesses now see cyber security as a high priority, an increase of 12% since 2016.[7] The introduction of the Network & Information Systems Regulations ('NIS regulations') in 2018 also led to designated organisations taking measures to better ensure the security of their networks and information systems, leading to a reduction in the cyber risks posed to essential services and important digital services.[8] A good example of collaboration across the four nations of the UK has been the improvements made across the health sector, including the implementation of the NIS regulations.

**22.** We have provided comprehensive cyber security advice and guidance to organisations in the wider economy, and tailored support to critical sectors during the coronavirus (COVID-19). For the public, our Cyber Aware campaign has provided advice on the steps they can take to protect themselves online. When cyber attacks have got through we have used our world-leading incident response capabilities to provide direct support in the most serious cases and our investment in local law enforcement specialists means that every reported incident now receives a response.

**23.** We have established specialist law enforcement cyber units the UK, and alongside this the cyber PROTECT network, Economic Crime Victims Care Unit and regional Cyber Resilience Centres. These initiatives mean that for citizens and small-to-medium-sized organisations there is someone nearby or easily contactable who has the right skills and local knowledge to provide support and guidance to improve your cyber resilience.

**24.** However, we have growing evidence of gaps in our national resilience, with levels of cyber crime and breaches affecting government, businesses and individuals continuing to rise as well as cyber-enabled crime,

[3] NCSC, NCSC Annual Review 2021 (2021)
[4] DCMS, Code of Practice for Consumer IoT Security (2018)
[5] DCMS, ETSI industry standard based on the Code of Practice (2019)
[6] DCMS/RSM, The impact of GDPR on cyber security outcomes (2020); The General Data Protection Regulation (GDPR) that was introduced into UK law in 2018 has now been replaced by the UK GDPR)
[7] DCMS, Cyber Security Breaches Survey 2021 (2021)
[8] DCMS, Post-Implementation Review of the Network and Information Systems Regulations 2018 (2020)

like fraud.[9] [10] Legacy IT systems, supply chain vulnerabilities and a shortage of cyber security professionals are growing areas of concern. Almost four in ten businesses (39%) and a quarter of charities (26%) report suffering cyber security breaches or attacks in the last year, and many organisations (especially small and medium enterprises) lack the ability to protect themselves and respond to incidents.[11] Industry tells us that many businesses do not understand the cyber risks they face, that commercial incentives to invest in cyber security are not clear, and that there is often little motivation to report breaches and attacks.

## The UK's international leadership and influence

**25.** Internationally, UK cyber expertise is regarded highly by our partners and the UK has been instrumental in increasing international capability and resolve to confront malicious cyber activity. This has been reinforced by responsible use of our offensive cyber capabilities, consistent with both UK and international law and our publicly stated positions, in contrast with the indiscriminate activities of some of our adversaries.

**26.** During our period as Chair-in-Office of the Commonwealth, the UK conceived and led the implementation of the Commonwealth Cyber Declaration, a shared commitment to our security, prosperity and values in cyberspace. The National Crime Agency's (NCA) international network has strengthened our cyber law enforcement partnerships overseas, building on relationships cultivated through a long history of collaborative operational response. The UK has also grown its overseas network of cyber and tech security officers across five continents and undertaken capacity building work across 100 countries, building resilience, enhancing UK influence and promoting UK values.

**27.** The Cyber Security Ambassador programme has developed long-term relationships and helped UK businesses secure major international contracts. UK international development interventions such as the Digital Access Programme have successfully collaborated with partner countries in Africa, Asia and Latin America by providing technical advice to enhance the cybersecurity capacity of their government, business sectors and users – including through increasing cyber-hygiene skills in underserved communities to enable the most vulnerable to protect themselves from the risks and challenges of being online

**28.** However, we face competing approaches internationally as systemic competitors like China and Russia continue to advocate for greater national sovereignty over cyberspace as the answer to security challenges. Internet freedom is decreasing globally and the vision of the internet as a shared space that supports the exchange of knowledge and goods between open societies risks coming under threat.

[9] Defined as Computer Misuse Act offences
[10] ONS, Crime in England and Wales: year ending June 2021 (2021)
[11] DCMS, Cyber Security Breaches Survey 2021 (2021)

## Countering cyber threats to the UK and deterring our adversaries

**29.** The threats we face in and through cyberspace have grown in intensity, complexity and severity in recent years. Cyber attacks against the UK are conducted by an expanding range of state actors, criminal groups (sometimes acting at the direction of states or with their implicit approval) and activists for the purpose of espionage, commercial gain, sabotage and disinformation. Such attacks cause significant financial loss, intellectual property theft, psychological distress, disruption to services and assets and risks to our critical national infrastructure, democratic institutions and media. They can also damage investor and consumer confidence and amplify existing inequalities and harms. During the COVID-19 pandemic the shadow pandemic of gender-based violence was compounded by online attacks. Ransomware attacks continue to become more sophisticated and damaging. While the overall level of cyber threat from hostile actors during the COVID-19 pandemic has remained constant, they have exploited it as an opportunity and shifted their cyber operations to steal vaccine and medical research, and to undermine other nations already hampered by the crisis. The growing dependence on digital technologies for remote working and online transactions has also increased exposure to risks. Alongside this, digital divides have also created uneven access to online services and exposed people to online abuse and harms due to limited digital literacy and awareness of the cyber security measures we can all take to stay secure online.[12]

**30.** Government has taken steps to counter these growing threats. Significant investment in our intelligence capabilities has increased our understanding of the threat and enabled us to conduct more effective covert counter campaigns. We have developed an integrated law enforcement response to cyber crime, led by the National Crime Agency (NCA) and dedicated cyber teams within regional organised crime units and local police forces across England, Wales, Northern Ireland and Scotland. This has enhanced our operational and investigative edge over cyber criminals and other adversaries. The government is also strengthening the security of the increasing number of digital identity solutions, by developing the UK digital identity and attributes trust framework.[13] This will also help to tackle crimes that involve misuse of identity data. And the NCA's Cyber Choices programme is helping people to make more informed choices, diverting them from criminality to use their cyber skills in a positive and legal way.

**31.** We have invested significantly in our offensive cyber capabilities, first through the National Offensive Cyber Programme, and more recently through the establishment of the National Cyber Force (NCF). The NCF draws together personnel from the Government Communications Headquarters (GCHQ), the Ministry of Defence (MOD), the Secret Intelligence Service (SIS, also known as MI6) and the Defence Science and Technology Laboratory, under one unified command for the first time. It is operating in and through cyberspace to keep the country safe and to protect and promote the UK's interests at home and abroad.

[12] NCSC, CyberAware

[13] DCMS, UK digital identity and attributes trust framework (2021)

**32.** In coordination with our allies, we have also sought to raise the cost of state-sponsored hostile activity in cyberspace by attributing attacks – as we did with the recent SolarWinds and Microsoft Exchange breaches – and imposing consequences on those responsible. The development of the autonomous UK cyber sanctions regime has added another disruptive tool that we have used to respond to incidents such as the WannaCry and NotPetya attacks. However, despite all this, our approach to cyber deterrence does not yet seem to have fundamentally altered the risk calculus for attackers. Some recent examples of significant cyber attacks are described below.

# Recent case studies of cyber attacks

During 2021, the UK 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.

## Cyber criminals using ransomware to attack public services

Ransomware became the most significant cyber threat facing the UK in 2021. Due to the likely impact of a successful attack on essential services or critical national infrastructure the NCSC assessed ransomware as potentially as harmful as state-sponsored espionage.[14]

In October 2020, Hackney Council suffered a ransomware cyber attack which caused many months of disruption and cost millions of pounds to rectify. At a critical time when it was dealing with the impact of the COVID-19 pandemic, the council was locked out of important data and many services were disrupted, including council tax and benefit payments. Other local authorities have suffered similar attacks, as have a variety of organisations in the education sector.

[14] NCSC, Mitigating malware and ransomware attacks (2021)

In May 2021, a ransomware attack against the Irish Health Service Executive (HSE) disrupted Irish healthcare IT networks and hospitals for over 10 days, causing real-world consequences to patients and their families. Some stolen patient data was also published online. The HSE, which provides health and social care services in Ireland, shut down national and regional networks the same day to contain the incident. Malicious cyber activity was also detected on the Irish Department of Health (DoH) network however due to the deployment of tools during the investigation process an attempt to execute ransomware was detected and stopped. The attack also had an impact on Northern Ireland, affecting the ability to access data held by HSE for some cross-border patient services.

Importantly, no ransom payment was made in either case. **Law enforcement do not encourage, endorse, nor condone the payment of ransom demands. If you do pay the ransom:**

- **there is no guarantee that you will get access to your data or computer**
- **your computer will still be infected**
- **you will be paying criminal groups**
- **you're more likely to be targeted in the future**

The NCSC publish guidance on how to defend organisations against malware or ransomware attacks, including how to prepare for an incident and steps to take if your organisation is already infected.

## States exploiting strategic vulnerabilities and supply chains

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 early December 2020, a US cyber security firm, FireEye, found that an attacker had been able to add a malicious modification to a product that they and many other organisations around the world utilise. This modification allowed the attacker to send administrator-level commands to any affected installation of that product and could be used for further targeted attacks on connected systems. The initial supply chain attack was conducted through a piece of software called Orion, an IT network monitoring tool developed by a company called **SolarWinds**. The actor was able to implant malicious code into an update file for the software, as far back as March 2020. In April 2021 the NCSC, together with its security counterparts in the US, revealed for the first time that Russia's Foreign Intelligence Service (the SVR) was behind this attack – one of the most serious cyber intrusions of recent times.[15] SolarWinds confirmed 18,000 organisations across the world

[15] FCDO, Russia: UK and US expose global campaign of malign activity by Russian intelligence services (2021)

including US Government departments were affected. This incident was part of a wider pattern of cyber intrusions by the SVR who have previously attempted to gain access to the IT networks of NATO members and governments across Europe.

On 2 March 2021, Microsoft made public that sophisticated actors had attacked a number of **Microsoft Exchange** servers, which are used by organisations worldwide to manage their email, scheduling and collaboration. Microsoft assessed that the initial intrusions commenced as early as January 2021 and were Chinese state-sponsored. In response to this they released multiple security updates for affected servers. In July 2021, the UK joined like-minded partners to confirm that Chinese state-backed actors were responsible for the attacks that affected over a quarter of a million servers worldwide.[16] The attack was highly likely to enable large-scale espionage, including acquiring personally identifiable information and intellectual property. Compromising Microsoft Exchange gave the perpetrator a foothold to pivot further into the IT networks of victims. At the time of the attack, the government quickly provided advice and recommended actions to those affected and Microsoft said that by end of March that 92% of customers had patched against the vulnerability.

[16] FCDO, UK and allies hold Chinese state responsible for a pervasive pattern of hacking (2021)

## Drivers of change

**33.** The coming decade will see the **continued rapid expansion of data and digital connectivity to almost every aspect of our lives**. Huge global growth in Internet access and usage, underpinned by data and the infrastructure upon which data use relies, is creating new markets and increasing convenience, choice and efficiency. But it also makes countries much more dependent on interconnected digital systems, providing more opportunities for malicious activity and significant 'real-world' impact. As critical and non-critical technologies continue to converge across sectors these risks are spreading to new areas of our economy, and the movement of data and services into the cloud – and often out of the UK – is further increasing our exposure.

**34.** We are increasingly seeing the interaction of established businesses in regulated sectors, such as telecoms and energy, with new and largely unregulated businesses, such as those providing microgeneration, electric vehicle charging or 'connected places' capabilities. Critical infrastructures will become much more distributed and diffuse and this fundamentally changes how regulation will impact the security of the critical functions and services we rely on. This diversification will also affect our wider national security, making it more difficult to gain access to information whether for law enforcement or cyber security. This change in environment will also affect products and services more widely outside of our traditional critical national infrastructure.

**35.** This **increasingly complex landscape** will make it even harder for states, businesses and society to understand the risks they face and how they can and should protect themselves. Increased dependency on third party suppliers of managed services, which often have privileged access to the IT systems of thousands of clients, is creating new risks that need to be addressed. Devices and networks will increasingly be connected to the internet as standard, extending cyberspace to our homes, vehicles, built environment and industrial infrastructure. Sensors, wearables, medical devices and biometrics will further blur the boundary between offline and online activity. Cyber risks will become pervasive, increasing the volume of personal and sensitive data generated and the potential impact if systems are breached.

**36.** Against this backdrop, the **threats in cyberspace will continue to evolve and diversify** as high-end cyber capabilities become commoditised and proliferate to a wider range of states and criminal groups. The number of actors with the ability and intent to target the UK in cyberspace will increase and states will employ a wider range of levers to conduct disruptive activity, including the use of proxy actors. The accelerated transition to hybrid working and restrictions on international travel resulting from the pandemic have led to greater reliance on digital services and incentivised organised crime groups towards cyber crimes. We are already beginning to see signs of this trend with the latest crime survey estimating that cyber crimes have increased significantly between 2019 and 2021.[17]

[17] ONS, Crime in England and Wales: year ending June 2021 (2021)

This challenge will not be unique to the UK, creating mutual vulnerability for all those who rely on cyberspace.

**37. Cyberspace will become more contested** as state and non-state actors seek strategic advantage in and through cyberspace. Cyber operations will become increasingly important to power projection below the threshold of armed conflict and in pre-conflict situations. Future conflicts will also see an increase in the use of cyber capabilities. For the UK to act effectively we will require higher levels of cyber resilience in our defence capabilities. Cyber operations will need to be integrated with other force elements to defeat threats and enable wider defence activity. Space will increasingly become a domain of activity, as set out in the National Space Strategy, opening up new areas of risk but also creating opportunities for the UK to exploit its cyber capabilities to achieve advantage in new ways.[18]

**38.** Debates over the rules governing cyberspace will increasingly become a site of **systemic competition between great powers,** with a clash of values between countries that want to preserve a system based on open societies and systemic competitors like China and Russia who are promoting greater state control as the only way to secure cyberspace. This will put pressure on the free and open internet, as nation states, big technology firms and other actors promote competing approaches to technical standards and internet governance.

**39.** This will be exacerbated by **competition for control of a rapidly evolving technological landscape**. As digital technology is integrated into our everyday lives, businesses and infrastructure, some technologies are becoming genuinely critical to the functioning of society. Power will increasingly be held by countries that have a strategic advantage in science and technology and access to the data that drives innovation, enabling them to exert influence over others and to shape global standards in ways that best fit their own economic and political interests.

**40. Emerging technologies** such as digital twins, quantum computing, and large-scale autonomous systems – and the information they generate – will create new opportunities and risks and open up new cyber capabilities for attackers and defenders, just as cryptocurrencies are being exploited by ransomware gangs. Leadership in technology is becoming more distributed, and the UK will not be able to develop sovereign capability in all the technologies that matter. States and companies make use of technical standards to promote their own interests and we risk key technologies being shaped by those who do not share our values.

**41.** For over a decade the UK has pursued an ambitious national cyber security strategy and sustained a significant level of investment, establishing the country as a global leader in cyber. As evident from the analysis above, significant challenges and opportunities remain. The following sections outline our national response.

[18] HMG, National Space Strategy (2021)


#CyberFirst
ncsc.gov.uk/new-talent
CAREERS
This is a CyberFirst world. Train for it.
University bursary and degree apprenticeship
National Cyber Security Centre

# Our National Response

**42.** In this strategic environment, the UK has a choice to make. We could aim simply to keep pace with the threats and challenges we face in an increasingly complex cyberspace, consolidating the progress of the last five years and addressing the most urgent issues where we can. There are two risks to this approach. The first is that we do not fully realise the potential of the UK's strength in cyber to support national priorities, and miss out on opportunities. The second, more severe risk is that we reach a technological tipping point, and find that the foundations of our future economy and society are being shaped by our competitors and adversaries, and that we will have to work harder to assure our own security.

**43.** Our judgment is that, as cyberspace becomes ever more fundamental to our interests and those of our allies and adversaries, **it is a strategic imperative to foster our competitive advantage in navigating this landscape**. This will enable us not only to assure our security today but also to shape and benefit from the world of tomorrow.

## Our vision, goals and principles

**44.** Our vision is that the UK in 2030 will continue to be a **leading responsible and democratic cyber power, able to protect and promote our interests in and through cyberspace in support of national goals**.

**45.** To realise this vision we will pursue five strategic goals. Each aims to bolster our national strength in one of the five dimensions of cyber power, and collectively they aim to enhance our ability to uphold a cyberspace that reflects our values and interests. These five goals – or pillars – form a strategic framework to guide our activity, and Part 2 sets out the actions we will take to 2025 under each one.

- **Pillar 1: Strengthening the UK cyber ecosystem**, investing in our people and skills and deepening the partnership between government, academia and industry
- **Pillar 2: Building a resilient and prosperous digital UK**, reducing cyber risks so businesses can maximise the economic benefits of digital technology and citizens are secure online and confident that their data is protected
- **Pillar 3: Taking the lead in the technologies vital to cyber power,** building our industrial capability and developing frameworks to secure future technologies
- **Pillar 4: Advancing UK global leadership and influence for a more secure, prosperous and open international order**, working with government and industry partners and sharing the expertise that underpins UK cyber power
- **Pillar 5: Detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace**, making more integrated, creative and routine use of the UK's full spectrum of levers

**46.** These goals are intended to be mutually reinforcing. For example, achieving higher levels of cyber security and resilience domestically will be a necessary foundation for a more active stance internationally. In turn, our global supply chains and the threats we face from overseas mean we will not be able to assure our own security without more actively shaping the behaviour of international actors. And our ability to influence global debates on cyberspace, the internet and technology will rely on maintaining our technical edge and building an innovation ecosystem that generates genuine advantage in the technologies that matter most.

**47.** Central to our vision is the **promotion of a free, open, peaceful and secure cyberspace**. Our strategic focus on cyber power is not about stoking conflict or setting the UK up to win a zero-sum game. As the Integrated Review identifies, a world in which open societies and economies can flourish is the best guarantor of our future prosperity, sovereignty and security. The UK will work with like-minded nations to promote our shared values of openness and democracy, pursuing a **responsible, democratic approach to cyber power**. This means that in working towards these five strategic goals we will apply the following **principles**:

- We will prioritise the ability of citizens and businesses to operate in cyberspace safely and securely so they can maximise the economic and societal benefits of digital technology and exercise their legal and democratic rights

- We will work to uphold an open and interoperable internet as the best model to support global prosperity and wellbeing, resisting the pressure of authoritarian states towards fragmentation and their idea of internet sovereignty
- We will make lawful, proportionate and responsible use of our cyber capabilities, supported by clear oversight and engagement with the public and our allies, and we will hold others to account for reckless or indiscriminate behaviour in cyberspace
- We will take action against the criminal use of cyberspace by all means available, calling out those who use criminal proxies or harbour criminal groups in their territories and working to prevent the proliferation of high-end cyber capabilities to criminals
- We will champion an inclusive, multi-stakeholder approach to debates about the future of cyberspace and digital technology, upholding human rights in cyberspace and countering moves towards digital authoritarianism and state control

## Key shifts in our approach

**48.** In many areas our strategy will build on our current approach, seeking to enhance, expand or adapt our efforts where necessary. The main distinctions from the National Cyber Security Strategy 2016-2021 are set out below and reflect our broader ambition to cement the UK's position as a leading cyber power.

**49. A commitment to keeping the UK at the cutting edge on cyber.** The government will be investing £2.6 billion in cyber and legacy IT over the next three years. This is in addition to significant investment in the National Cyber Force announced in Spending Review 2020 (SR20). It includes a £114 million increase in the National Cyber Security Programme; and is alongside increases in investment also announced in research and development (R&D), intelligence, defence, innovation, infrastructure and skills, all of which will contribute in part to UK cyber power. Investment in cyber announced in SR20 and Spending Review 2021 (SR21) far exceeds the £1.9 billion over five years committed to the previous strategy.[19]

**50. A more comprehensive National Cyber Strategy.** Cyber security remains at the heart of this strategy, but it now draws together the full range of the UK's capabilities inside and outside government. It gives greater weight to the critical technologies and infrastructure that underpin cyberspace, supports UK cyber companies both to grow domestically and compete internationally, steps up international action to shape and influence the future of cyberspace, and integrates offensive cyber as a lever of power. It calls for a truly joined up, national strategic approach. The strategy distributes responsibilities for leadership and coordination across Secretaries of State, and much more closely involves the devolved administrations. This builds on our success at coordinating effort across government, which is a key UK strength.

[19] HM Treasury, Autumn Budget and Spending Review 2021 (2021)

**51. A whole-of-society effort.** Our aim is for a national strategic approach that is shaped by and helps guide decision-making in organisations across the country; and provides the basis for stronger collaboration with our partners in the UK and around the world. There is more work to do to make this a reality. Short term actions will include: (i) establishing a new National Cyber Advisory Board, inviting senior leaders from the private and third sectors to challenge, support and inform our approach; (ii) reorienting our cyber sector innovation programmes away from large, often London-based initiatives to a regionally delivered model, built in partnership with local industry, innovators, law enforcement and academia; and (iii) taking steps to increase the diversity of the cyber workforce – recognising that being able to harness and nurture the skills and talents of the whole population is critical for our national security. The strategy itself has been informed by engagement with the devolved governments of Northern Ireland, Scotland and Wales, industry, law enforcement, regulators, academia, civil society and international partners. Our intention is to keep these dialogues open over the period of its implementation.

**52. A more proactive approach to fostering and protecting our competitive advantage in the technologies critical to cyberspace.** The Integrated Review and subsequent strategies have already begun to take this approach forward in areas such as artificial intelligence, quantum technologies and data. This strategy makes further commitments around secure microprocessor design, the security of operational technologies and cryptography. It announces the establishment of a national laboratory for operational technology security, as a new centre of excellence focused on building the highest level of cyber resilience in partnership with industry and academia. And it announces the expansion of the National Cyber Security Centre's (NCSC) research capabilities, including the new applied research hub in Manchester, with a focus on emerging technology in areas such as connected places and transport. The strategy also builds on our successful work to promote approaches that build security into new technologies, making them "secure by design". This will mean investing and making more use of regulatory and legislative levers where necessary to promote more diverse, secure and resilient technology supply chains, as we have done in telecoms.

**53. Significantly strengthening our core effort to promote cyber security, with government leading the way.** We will invest more than ever before in a rapid and radical overhaul of government cyber security, setting clear standards for departments and addressing legacy IT infrastructure. Government's critical functions will be significantly hardened to cyber attack by 2025 and we will ensure that all government organisations – across the whole public sector – are resilient to known vulnerabilities and attack methods by 2030. We will do more to protect and engage citizens while removing as much of the burden from them as possible. We will harden the digital environment, protecting citizens from cyber crime and fraud and placing more responsibility on manufacturers, retailers, service providers and the public sector to raise cyber security standards. We will drive up the level of private sector engagement and investment in cyber resilience by aligning regulations and incentives across the economy

and providing more support. We will also focus more on supply chain risks, testing a range of interventions to help organisations manage the cyber security risks posed by their suppliers, and ensure that best practice filters down through the supply chain.

**54. More integrated and sustained campaigns to disrupt and deter our adversaries and protect and promote the UK's interests in cyberspace.** These campaigns will draw on a fuller range of diplomatic, policy and operational levers across government. They will be significantly underpinned by the establishment and expansion of the National Cyber Force (NCF), which will be based in Samlesbury in Lancashire. We will make more routine use of the NCF's capabilities to disrupt threats from both state and non-state actors and to support the UK's wider national security interests. Our campaigns will also benefit from major new investment in high-end capabilities for law enforcement at national, regional and local levels. This will help us to tackle the substantial threat from ransomware and increasingly innovative cyber criminals. We will also continue to make use of the UK's autonomous cyber sanctions regime and attributions process to impose costs on our adversaries and call out malign and reckless and attacks.

**55. Putting cyber power at the heart of the UK's foreign policy agenda and recognising that every part of the strategy requires international engagement.** We will reinforce our core alliances and engage a broader range of countries to counter the spread of digital authoritarianism. Over the next few years, we will increase investment in international programmes to support partner countries, helping build their resilience and enhancing their abilities to counter cyber threats. And we will better leverage the full range of our domestic strengths, including operational and strategic communications expertise, thought leadership, trading relationships and industrial partnerships to support our international goals.

## Roles and responsibilities across the UK

**56.** Central to our strategy will be a whole-of-society approach to cyber. We need to build an enduring and balanced partnership across the public, private and third sectors, with each playing an important role in our national effort.

### Citizens

**57.** This strategy aims to remove as much of the burden of cyber security from citizens as possible but we will all continue to have an important role to play. Whilst the government will do as much as possible to stop cyber attacks before they cause harm to people, some threat actors will find a way to circumvent these protections. We can all take action to improve the security of the assets we value in both the physical and virtual worlds.[20] That means fulfilling our personal responsibility to take all reasonable steps to safeguard not only our hardware – our smartphones and other devices – but also the data, software and systems that afford us freedom, flexibility and convenience in our private and professional lives. To support this, the government provides technically accurate, timely and actionable advice. Civil society organisations and community groups also play a major role supporting people

[20] Cyber Aware is the government's advice on how to stay secure online

to understand and protect themselves from cyber risks. Many charities, for example, provide targeted support, advice and awareness-raising to vulnerable groups.

## Businesses and organisations

**58.** Businesses and organisations have a responsibility to ensure they are effectively managing their cyber risks, to become cyber resilient and to support their customers and the people who use their services. Businesses and organisations are increasingly dependent on digital technologies and online services to operate, innovate and grow. This improves services but also creates new risks and challenges, such as the ever increasing volume of personal data and digital assets which they are responsible for. This brings a responsibility to protect those data and assets, while maintaining services. Failure to do so can have significant reputational and economic implications for organisations and cause harm to their customers. Operators of essential services and providers of key digital services (such as cloud services) have particular responsibilities to address the cyber risks they face and meet the obligations set out in the Network & Information Systems Regulations ('NIS regulations'). Advice and guidance from the NCSC helps to provide support to all businesses and organisations to help them protect their information, assets and systems. The Information Commissioner's Office (ICO) also provides advice for organisations on their cyber security obligations under the UK General Data Protection Regulation.

## The cyber security sector and major technology companies

**59.** The UK's growing cyber security sector has a critical role in responding to the emerging cyber threats and challenges that face our country. The rapid proliferation of connectable products and the accelerated digital transformation of businesses and organisations are providing opportunities for the sector to grow and innovate, providing new services and products. This strategy describes how the government will continue to support the growth of the UK cyber security sector and benefit from their capabilities and expertise by maintaining and strengthening our partnerships. We also want to strengthen the broader partnerships between academia, the wider technical community and the private sector, to ensure that we capitalise fully on the UK's technical expertise and know-how.

**60.** The major technology companies that provide digital services have a crucial role to play in ensuring a secure environment for UK businesses and organisations to operate in. This is particularly true for the managed service providers and platform businesses that integrate a number of activities. They need to ensure the services they offer are 'secure by default' and are not overly dependent on their customers taking protective actions. Major technology companies also have a particular responsibility to prioritise their own cyber resilience. The increasing dependency of businesses, government and wider society on cloud and online services is creating new and unique vulnerabilities and interdependencies.

## Government

**61.** The **UK government** is uniquely positioned to bring together the intelligence necessary to understand the most sophisticated threats, make and enforce the law, set national standards, and counter threats from hostile actors including conducting offensive cyber operations. Through this strategy we will invest in strengthening our national cyber capabilities. Government departments and public sector bodies are also responsible for protecting their own networks and systems. As the holder of significant data and a provider of services, the government takes stringent measures to provide safeguards for its information assets. Lastly, the government also has an important responsibility to advise and inform citizens, businesses and organisations what they need to do to protect themselves online. Where necessary this includes setting the standards we expect key companies and organisations to meet in order to protect all of us.

**62.** Most areas of cyber policy and the majority of measures outlined in this strategy relate to reserved matters such as national security, foreign affairs and defence, telecommunications, product standards and safety, and consumer protection. But the development and implementation of this strategy still depends on input, action and investment by **the devolved governments of Northern Ireland, Scotland and Wales**. This is especially true where this relates to devolved policy areas which sit primarily within the 'ecosystem' and 'resilience' pillars of this strategy, such as education, policing and the cyber resilience of certain critical sectors including their own public sectors. Coordination and cooperation across the four nations of the UK is essential to ensure the greatest impact across the whole country. This requires regular and early engagement by the Cabinet Office and other UK government departments with their Welsh, Scottish and Northern Irish counterparts to share information on priorities and plans. This also helps to avoid duplication and get the best value from public funding. The devolved governments will continue to develop their own cyber strategies and plans, aligning them with this UK government strategy.

# The National Cyber Security Centre

***"Helping to make the UK the safest place to live and work online"***

The National Cyber Security Centre (NCSC) was formally launched in 2017, as part of GCHQ, to be the UK's national authority on the cyber security environment: sharing knowledge, addressing systemic vulnerabilities and providing leadership on key national cyber security issues.[21] The NCSC's establishment simplified the government's operational structures, transformed the UK's ability to respond to national-level cyber incidents, and initiated the roll-out of innovative digital services that have helped to make organisations and individuals automatically safer online.

We are making sure that the NCSC is fit for the challenges of the next decade by clarifying the enduring capabilities and attributes that underpin its work, funding them on a sustainable basis, and focussing their use where operating experience to date tells us they will have the maximum possible impact at a national scale.

The enduring capabilities and attributes that underpin the NCSC's work are:

- World-class technical expertise in the cyber security disciplines and specialisms the UK needs;
- Unparalleled insight into current and potential cyber threats – intent and capability – to UK interests;
- Access to the full range of UK national security capabilities and authorities for cyber security goals;
- Direct reach into cyber security communities in conjunction with partners in academia, industry, and internationally;
- Cryptographic capabilities and services, crucial to the safety and security of UK interests globally.

The NCSC's principal responsibilities under the new strategy will be to:

- **Take direct action to reduce cyber harms to the UK** by providing protection at scale through digital services (e.g. Active Cyber Defence), driving changes in technology, managing the response to nationally-significant cyber incidents, and – with the National Cyber Force (NCF) – directly countering the cyber operations of our adversaries.

[21] HMG, National Cyber Security Strategy 2016 to 2021 (2016): paragraph 1.9

- **Support all parts of UK society to protect themselves** by providing tailored expertise and unique knowledge that citizens, businesses and organisations across the UK can use to protect themselves and help make the UK a safer place for everyone online.
- **Providing technical input to HMG policy and regulation on the issues of most importance for cyber security** by providing policy leads across Whitehall with authoritative technical input and threat assessment derived from the NCSC's core capabilities, supporting development and implementation of policies and regulations to keep the citizens, organisations and interests digitally secure.
- **Providing UK sovereign capabilities** through the NCSC's National Crypt-Key Centre, which protects the critical information and services on which the UK military and national security community rely, including from attack by our most capable adversaries.
- **Supporting growth in cyber skills and investment** by providing the technical underpinning for every level of cyber education and engaging and supporting industry, catalysing investment into the cyber sector.

The NCSC will also contribute to the **evaluation of progress** against the objectives of this national cyber strategy through NCSC Assessments, the UK's editorially-independent cyber assessments function.

# The National Cyber Force

Established in 2020, the National Cyber Force (NCF) is responsible for operating in and through cyberspace to counter, disrupt, degrade and contest those who would do harm to the UK or its allies, to keep the country safe and to protect and promote the UK's interests at home and abroad. The NCF is made up of a roughly equal share of personnel from defence and intelligence and brings together their expertise, resources and authorities under a single command structure. It will be based in Samlesbury, Lancashire.

The NCF delivers a broad range of outcomes in the interests of national security, such as support to defence, the UK's economic wellbeing and the prevention of serious NCF activities range, from the tactical through to the strategic, against both state actors and non-state actors. Its work falls into three main categories:

- Countering threats from terrorists, criminals and states using the internet to operate across borders in order to do harm to the UK and other democratic societies
- Countering threats which disrupt the confidentiality, integrity and availability of data and services in cyberspace (i.e. supporting cybersecurity)
- Contributing to UK Defence operations and helping deliver the UK's foreign policy agenda (for example intervening in a humanitarian crisis to protect civilians)

NCF operations can be used to influence individuals and groups, disrupt online and communications systems and degrade the operations of physical systems. This type of activity is often referred to as offensive cyber (OC).

NCF operations are conducted in line with a well-established legal framework, which includes the Intelligence Services Act 1994 and the Investigatory Powers Act 2016. The UK has previously made it clear that it develops and deploys capabilities in accordance with international law, including the law of armed conflict where applicable. Its activities are subject to ministerial approval, judicial oversight and Parliamentary review, making the UK's governance regime for cyber operations one of the strongest in the world.

The UK will not routinely talk about individual cyber operations, but the kinds of operational activity the NCF could conduct include:

- Stopping terrorist groups from carrying out their plans by disabling their command and control communications and limiting the dissemination of extremist media
- Reducing the risk of harm to UK armed forces by degrading adversary weapons systems
- Defending democracy and free, fair and open elections by countering organised state disinformation campaigns intended to undermine them
- Preventing criminal groups from profiting from their activities by disrupting their use of online platforms and services
- Helping to enforce international sanctions by disrupting efforts to evade them
- Shielding the UK and others from cyber attacks by disrupting the infrastructure used by adversaries to carry them out
- Protecting civilians in a humanitarian crisis by preserving their ability to access critical information

As the national centre of excellence for effects operations in and through cyberspace the NCF will transform the UK's ability to develop, integrate and utilise these capabilities alongside others and optimise them to deliver effect.

# Law Enforcement's National Cyber Crime Network

Established over the course of the National Cyber Security Strategy 2016-2021, law enforcement's national cyber crime network has developed a fully integrated response to cyber crime, ready to deliver an intelligence-led response to all forms of cyber attacks against individuals, organisations or whole sectors. This is a nationwide system operating at national, regional and local levels. It provides victim care, helps businesses and people to be protected and to recover swiftly, and pursues criminal justice outcomes against perpetrators.

The **National Crime Agency's (NCA) National Cyber Crime Unit (NCCU)** provides national leadership and coordination of the response, supported by a network of dedicated **Regional Cyber Crime Units (RCCUs)** in each of England and Wales's nine police regions, in partnership with their counterparts in Police Scotland and Police Service of Northern Ireland, as well as the Metropolitan Police Service's Cyber Crime Unit.

These are further complemented by dedicated **Local Cyber Crime Units (LCCUs)**, embedded in each of the 43 police forces and synchronised through a regional coordinator. These Regional and Local CCUs can investigate and pursue offenders, help business and victims protect themselves from attack and work with partners to prevent vulnerable individuals from being drawn into committing cyber crime.

Centralised crime reporting, triage and analysis is provided through **Action Fraud**, hosted by the **City of London Police**. The most serious and/or complex cases are subsequently referred to the NCA and regional network to pursue, while other cases are disseminated to local forces. The City of London Police also coordinate victim support, including through the **Economic Crime Victim Care Unit.**

Systems are being joined up with transformed forensic, intelligence and data-sharing capabilities to build a single platform so that national and regional units can access all the specialist high-end capabilities and tools being developed. This includes the ability to collaborate effectively with partners in the security and intelligence community, in particular to respond to blended criminal and state threats. Continuing the ethos of 'build it once, build it nationally for the benefit of the whole cyber crime network', these

capabilities can also be accessed by the local cyber crime units through the regional coordinators. This whole system approach is already delivering a significantly enhanced response to the cyber crime threat.

The law enforcement Cyber Crime Network will continue to drive our criminal justice response to malicious activities in cyberspace regardless of the threat actor at the international, national, regional and local level. This will be complimented by a range of other disruptive methods including but not limited to:

- Developing specialist high end investigative and disruptive cyber capabilities
- Utilising the NCA's extensive international network to support partner country interventions with intelligence and evidence
- Preventing criminal groups from profiting from their activities by disrupting their use of criminal marketplaces and enabling services
- Protecting the UK and other countries from cyber crimes by degrading and disrupting the infrastructure used to carry them out
- Contributing to sanction activity and public attribution against high echelon offenders
- Seizing cryptocurrency and other assets as the proceeds of cyber crime

# Part 2:
# Implementation

# Pillar 1:
# UK Cyber Ecosystem

# Strengthening the UK's cyber ecosystem

**63.** For this strategy to succeed we need to ensure that the UK has the right people, knowledge and partnerships. We must have a diverse and technically skilled workforce, a vibrant research community, an internationally competitive cyber sector and a thriving regional innovation ecosystem that enables us to take the lead in critical technologies, all built on stronger partnerships between government, industry and academia.

**64.** The growth of the cyber ecosystem needs to be self-sustaining, not dependent on government interventions. Over the course of this strategy we will transition from funding a range of largely bespoke and centrally-managed skills and innovation programmes, to a more sustainable, systemic and regional approach. We will build on the government's wider reforms to the skills and education systems to support and inspire more people to gain the skills they need to pursue a cyber career. And we will prioritise a range of concrete actions to increase the diversity of the cyber workforce. This is not only about ensuring that these jobs and careers are made available to everyone but also mission critical for our national security, ensuring we harness the talent and skills of the whole population. We will also ensure that cyber sector growth benefits the whole of the UK, not just London and the South East which is home to an estimated 45% of sector employment and accounts for 85% of external investment.[22]

**65.** Overall we will take on a more strategic role where we facilitate the coming together of industry leaders, academics, innovators, law enforcement, the national security community and others who want to collaborate on making the UK more resilient against cyber threats. We will align all the levers of government to support the cyber ecosystem, from how cyber is taught in schools to how economic regulations drive up standards, to ensure that the UK grows the vital capabilities necessary to secure ourselves against future threats.

[22] DCMS, Cyber Security Sectoral Analysis 2021 (2021)

## Objective 1: Strengthen the structures, partnerships and networks necessary to support a whole-of-society approach to cyber

**66.** Cyber power requires a whole-of-society approach. Our competitive advantage will come from our ability to nurture and harness talent across the UK and get the right people working together in the right ways across the whole public sector, industry and academia, pulling together the whole cyber community. We will need to form a genuine integrated delivery partnership with industry and ensure a broad geographic approach across the nations and regions of the UK, working closely with the devolved governments of Northern Ireland, Scotland and Wales and seizing the levelling up opportunity that cyber power presents. We will achieve the following outcomes by 2025:

**67. A more inclusive and strategic national cyber dialogue** with industry, academia and citizens by establishing a new senior National Cyber Advisory Board and building on the already strong networks of cyber growth and resilience partnerships and the academic centres of excellence for cyber security research and education

**68. More integrated and effective regional cyber networks across the UK**, enabling stronger partnerships between government, businesses and academia to support sectoral growth and business resilience. We will work with regional cyber clusters and the recently established UK Cyber Cluster Collaboration (UKC3), the growing number of regional cyber innovation centres and Cyber Resilience Centres, strengthening links between local businesses, academic centres of excellence and law enforcement.

**69.** These steps will build on the range of existing relationships between the National Cyber Security Centre (NCSC) and its stakeholders, between government departments, arm's-length bodies and the sectors of the economy they represent, including CNI and regulators, and the government's wider dialogue with industry and the digital and technology sectors.

## Ciara Mitchell, Head of Cyber at ScotlandIS

Ciara is also the manager of Scotland's Cyber Cluster and a board member of UKC3.

"Scotland's Cyber Cluster has played a key role in supporting the cyber security community in Scotland. There is a growing understanding of the expertise in Scotland on cluster management and the opportunity to build on a thriving cyber sector. As the value of clusters has become more recognised, I have been delighted to take on a key role in the new UK Cyber Cluster Collaboration as Ecosystem Development Lead. Through UKC3 there will be a greater focus on collaboration, innovation and skills development which provides a platform to grow the UK cyber security sector."

# Cyber Organisations (Locations representative)

**UK Cyber Clusters**

1. Bristol and Bath Cyber
2. Cyber North
3. Cyber Wales
4. CyNam (Cyber Cheltenham)
5. East of England Cyber Security Cluster
6. Midlands Cyber
7. ScotlandIS Cyber
8. South West Cyber Security Cluster
9. Yorkshire Cyber Security Cluster
10. NI Cyber (Northern Ireland)
11. North West Cyber Security Cluster
12. West of England Cyber Cluster

Academic Centre of Excellence in Cyber Security Education

Change Academic Centre of Excellence in Cyber Security Research*

GCHQ / NCSC site

Devolved Authority Organisations

*Red dot and black line denotes both CSE and CSR status

1 The Business Resilience Centre for the North East

2 The North West Cyber Resilience Centre

3 The Cyber Resilience Centre for the East Midlands

4 The Cyber Resilience Centre for the West Midlands

5 The Cyber Resilience Centre for the South East

6 The South West Cyber Resilience Centre

7 The Cyber Resilience Centre for Wales

8 The Eastern Cyber Resilience Centre

9 The Cyber Resilience Centre for London


Scottish Business Resilience Centre
Abertay University
CyberScotland Partnership
Edinburgh Napier University
University of Edinburgh
Queen's University Belfast
Northumbria University
Newcastle University
NI Cyber Security Centre
Lancaster University
GCHQ Scarborough
National Cyber Force
GCHQ Manchester
University of Birmingham
De Montfort University
NCSC Cheltenham
University of Warwick
University of South Wales
University of Cambridge
Cardiff University
University of Oxford
University of the West of England
University of Bristol
King's College London
GCHQ Bude
Imperial College London
University of Kent
University College, London
Royal Holloway
Kingston University
University of Surrey
University of Southampton

## Objective 2: Enhance and expand the nation's cyber skills at every level, including through a world class and diverse cyber security profession that inspires and equips future talent

**70.** Central to the UK's ambitions will be developing a sustained and diverse supply of highly-skilled people into the cyber workforce, capable of securing the core elements of the digital economy, as well as innovating and developing new approaches. This will support our aim to lead by example through recognising and retaining expertise across the public sector and increasing our capability in law enforcement, defence and security, including the National Cyber Force (NCF). As with other parts of this strategy we will work with the devolved governments of Scotland, Wales and Northern Ireland to ensure that a consistent approach is taken across the country on, UK government initiatives on devolved matters, such as education and skills. We will achieve the following outcomes by 2025:

**71. A significant increase in the number of people who have the skills they need to enter the cyber workforce**, building on the work happening across all four nations of the UK to ensure education and skills policy meets the demands of people and employers. We will do this through a number of measures including the expansion post-16 training programmes in line with the needs of the cyber workforce, funding a range of skills bootcamps in cyber security, the national rollout of the Institutes of Technology programme, and continuing the CyberFirst bursaries scheme for undergraduates. This builds on the government's work to align the majority of post-16 education and training with strengthened employer-led standards by 2030. These will be developed in conjunction with the UK Cyber Security Council for the wider cyber community and underpin apprenticeships, T Levels and new higher technical qualifications. This will ensure that employers have a central role in designing and developing qualifications and training.

**72. A higher quality and more established, recognised and structured cyber security profession**. Underpinned by Royal Charter the UK Cyber Security Council will establish professional standards and pathways into and through a cyber career, built on the world-leading Cyber Security Body of Knowledge (CyBOK). And we will explore all government levers, including legislation, to embed these standards across the profession, ensuring that excellence and expertise can be recognised clearly and consistently across the cyber workforce.

**73. A more diverse cyber workforce**, with underrepresented groups and those from disadvantaged communities across the UK given more effective support to enter into and flourish in a career in cyber. Our range of measures will include support for more women to enter the cyber workforce and specific interventions to support underrepresented groups to progress to senior levels. And we will build on the successes of extracurricular activities delivered through our flagship CyberFirst programme, including the CyberFirst Girls Competition. We will also increase access to education and career opportunities for at-risk young people through the National Crime Agency's Cyber Choices programme, diverting them away from illegal cyber activity towards more positive opportunities to make use of their talent and enthusiasm.

**74. A steady and diverse flow of highly-skilled people coming through our education system.** We will inspire and support more young people to follow a technology pathway through education, including an increase in the uptake and diversity of candidates taking Computer Science GCSE and equivalent qualifications in Scotland, and going onto further education such as T Levels in England and apprenticeships and higher education opportunities. And we will also upskill more teachers in England through the National Centre for Computing Education (NCCE), ensuring they have access to the resources and development opportunities that will help them spark interest in more students.

**75. Government is better able to identify, recruit, train and retain the cyber professionals it needs**. As major employers of cyber professionals, government and the public sector will need to lead by example, supporting and building on the measures outlined above. We will take a more coherent and effective approach across the public sector while also tailoring specific measures to upskill civil servants and senior leaders, and build our capability in defence and security including the NCF, the NCSC and law enforcement. This will include investment in early talent by expanding the Cyber Fast Stream and offering more cyber security apprenticeships, supporting specialist skills programmes within the NCA including graduate and intern placements, bespoke neurodiversity programmes and summer diversity programmes. It will build on the successes of the Defence Cyber School by expanding it into the Defence Cyber Academy with a broader offer of defensive and offensive cyber training, whilst collaborating with academic, industry and international partners.

# The UK Cyber Security Council

The UK Cyber Security Council launched in March 2021 and is a world first for the cyber security profession. Its mission is to be the voice of the profession, bringing clarity and structure to the growing cyber workforce and the range of qualifications, certifications and degrees that exist across the field. This is a vital step, recognising that the cyber profession incorporates a wide range of technical and non-technical expertise and specialisms across the economy, similar in breadth to more established professions such as medicine and law.

The Council has four aims:

- Thought leadership and professional standards: leading the work to develop and agree the standards that define cyber security
- Careers and learning: supporting employers and individuals as they make career decisions, with advice on cyber security skills, professional development and recognition
- Professional ethics: providing guiding principles within which practicing professionals and organisations themselves can demonstrate ethical practice in cyber security;
- Diversity and Inclusivity: promoting cyber security as a career opportunity for people of all ages and backgrounds, making efforts to remove barriers to entry and progression within the field

The Council will look to grow and establish its credibility and sustainability as the professional authority throughout the lifecycle of this strategy. It will bring together a range of existing professional and certification bodies, identifying and empowering expert organisations who can provide clarity over progression and competency requirements to new entrants, existing practitioners and employers alike.

The Queen approved the award of a Royal Charter to the UK Cyber Security Council in November 2021. This provides, for the first time, a bespoke chartered recognition specifically for cyber security, covering the range of specialisms that exist in the field.

We recognise there is more work to be done to embed professional standards and pathways across the cyber ecosystem, including across government, defence and law enforcement. The Council will play a major role in this, supporting young people and career changers to navigate their career in cyber.

### Simon Hepburn, CEO, UK Cyber Security Council

My work involves promoting the UK Cyber Security Council as "the voice for the cyber security profession." The Council is the self-regulatory body for the UK's cyber security profession, and we aim to unite the industry to develop, promote and steward nationally recognised standards for cyber to make the UK the safest place to live and work online. The Council was officially launched in March 2021 following a successful formation project, and we are now open for membership applications. The National Cyber Security Strategy is a crucial element to ensure that individuals and organisations can work in a manner which furthers the profession, with the Council a key coordinating player.

## Objective 3: Foster the growth of a sustainable, innovative and internationally competitive cyber and information security sector, delivering quality products and services, which meet the needs of government and the wider economy

**76.** To enhance our national cyber power and drive digital growth and exports, the UK needs a vibrant cyber sector made up of high quality, trustworthy companies. UK firms provide world-leading technologies, training and advice to both industry and governments in the UK and globally. But to develop cutting-edge technologies some companies need support and connections to investment to reach the stage where they can offer a viable product.

**77.** Companies also need to feel confident they are innovating in line with government approved parameters that other organisations are also following. And there is more we can do to help buyers navigate the complex landscape, with a huge range of products and services of varying quality. This will in turn stimulate demand in the ecosystem and support further growth. We will achieve the following outcomes by 2025:

**78. A cyber sector that has achieved greater than average global growth year on year**, including through trade and cyber exports. We will help cyber businesses to access new markets at home and overseas by supporting world-leading flagship cyber events in the UK and inviting our most innovative cyber businesses to participate in trade missions and international cyber fairs. And we will use public sector procurement more effectively and establish a comprehensive directory of NCSC accredited providers to encourage the demand for high quality cyber security products and services.

**79. An even more innovative cyber sector** that has seen a significant increase in early stage investment and more cyber businesses that have been able to launch, grow and scale. Our new Cyber Runway programme gives businesses a single focal point for support, learning lessons from our previous programmes such as the Tech Nation Cyber Programme, Cyber101 and Hut Zero. We will transform the Cheltenham Innovation Centre, which includes the cyber accelerator 'NCSC for Startups', into a true international centre of innovation: the National Cyber Innovation Centre. We will draw on the expertise of organisations that exist to promote and enable co-creation, such as the National Security Technology and Innovation Exchange. And we will encourage higher-risk investment in early stage cyber start-ups, including through the National Security Strategic Investment Fund, in partnership with the British Business Bank

**80. A UK cyber economy that has been levelled up significantly** with increased growth outside of the South East, contributing to recovery from the coronavirus (COVID-19) pandemic and supporting wider regional economic activity. We will establish the permanent headquarters of the NCF in Samlesbury, in the North West of England driving growth in the technology, digital and defence sectors outside of London and helping create new partnerships in the region. We will increase our support for innovators and entrepreneurs outside of London and the South East to develop their products and services, grow their businesses and recruit skilled staff. This includes the Golden Valley campus led by Cheltenham Borough Council dedicated to supporting the growth of cyber-related technology businesses. And we will increase the exporting capabilities of cyber companies across more regions of the UK through engagement with the regional cyber clusters and set piece events to showcase more of our cyber industry talent to international buyers.

**81. A greater number of companies able to offer cyber security technologies, products and services that meet independently verified quality standards**, increasing user confidence. We will deliver this in line with The Future of NCSC Technology Assurance white paper published by the NCSC in September 2021, using the NCSC brand and expertise to build a trusted marketplace that will help UK consumers buy services with confidence, improve their security and raise the national cyber security bar.[23]

[23] NCSC, White paper: The future of NCSC Technology Assurance (2021)

### Berta Pappenheim, CEO and founder, Cyberfish Company

CyberFish took part in a government cyber accelerator programme. Our mission is to help businesses and government teams prepare to better handle business disruptions, like cyber incidents. We do this by running incident simulation exercises with them, observing their team dynamics under stress, and coaching them on how to make improvements. Many advisors are good at either the technical side of incident response, or the behavioural side of leadership and decision-making. We do both, together, with expert knowledge from both sides. Our exercises have helped almost 500 industry leaders working in mission-critical teams across the globe to shift perspectives, improve their teamwork, leading to improved crisis response and decision-making.

# Interested in joining the cyber workforce or starting your own business?

**82.** Our previous strategy placed a major emphasis on growing the cyber skills base and cyber security services sector in the UK. As outlined in the strategic context we have made significant progress in **growing the sector and exports**:

Helping cyber businesses find international markets. The UK exported £4.2billion of cyber services in 2020.

Cyber Exchange, our online cyber portal, bringing together cyber businesses across all regions of the UK.

The Cyber Growth Partnership has been bringing government and industry together to break barriers to growth.

**83.** We have **supported innovators to grow and scale their businesses**, ensuring the UK cyber ecosystem has flourished over the last five years:

NCSC for Startups is pointing innovators towards the most important strategic challenges while its startups have already taken part in over 160 new corporate trials.

LORCA has helped 72 cyber innovators raise over £200 million in investment and earn over £37 million in revenue.

Cyber Runway supports innovators to launch, grow and scale their business – building on the success of Hutzero and Cyber101.

**84.** We have been working to narrow the annual shortfall of 10,000 professionals **entering the cyber workforce**:[24]

The CyberFirst bursary scheme supports undergraduate students and is delivering hundreds of individuals, with work experience, into the cyber workforce every year.

There are now four cyber apprenticeship standards that have been designed by industry and three cyber offerings for initial learning outcomes offered through the DfE 'Courses for Jobs' initiative.

There have been nine cyber bootcamps supported through the recent National Skills Fund, taking people into exciting cyber careers and more of these are planned for every year of the next spending period.

**85.** We have been **professionalising the cyber workforce**, making it more straightforward for organisations to understand what skills they need, and making it easier for individuals to navigate what they need to know:

The UK Cyber Security Council is a world-first professional authority for cyber security. It has begun to set clear and consistent professional standards, building on all the work that existing professional bodies have done to date. The Council will look to clearly identify effective qualifications from the myriad currently available.

The Cyber Security Body of Knowledge (CyBOK) informs and underpins education and professional training for the cyber security sector.

[24] DCMS, Understanding the cyber security recruitment pool (2021)

**86.** We have been working to **ensure that everyone can join the cyber workforce**, tackling inequality in the sector where only 16% are female, and only 3% of senior roles are held by women and ethnic minorities.[25]

The CyberFirst courses and Discovery programme have engaged nearly 300,000 young people aged 11-17 in the last five years.

The UK Cyber Cluster Collaboration is building partnerships between industry, schools and colleges to ensure opportunities and expertise are available across the regions.

The NCA's Cyber Choices programme is helping young people to make informed choices and use their cyber skills in a legal way, raising awareness and providing better alternatives such as apprenticeships and work placements

[25] HMG, Cyber security skillls in the UK labour market (2021)

# Pillar 2:
# Cyber Resilience

# Building a resilient and prosperous digital UK

**87.** Cyber security and resilience are foundational to our wider strategic aims as a cyber power: without them we cannot hope to take full advantage of the transformational potential of digital technologies to build back better, fairer and stronger, and to protect the UK's strategic advantage in and through cyberspace. We must continue building strong cyber defences, taking action to secure the UK's digital networks, information and assets at a national, local and individual level and ensure they are resilient when incidents occur.

**88.** And while we focus in this chapter on cyber resilience, to be fully effective this will need to form part of a holistic, whole-of-society endeavour to improve UK resilience. The forthcoming National Resilience Strategy, a key commitment of the Integrated Review, will set out the overarching approach to national resilience.

**89.** Significant progress has been made in the last decade in improving our cyber resilience, with the establishment of the National Cyber Security Centre (NCSC), increased availability of advice, guidance and other tools, and the implementation of legislation including the Network & Information Systems Regulations (NIS regulations), General Data Protection Regulation and Data Protection Act 2018. But serious gaps remain. Cyber breaches affect government, businesses, organisations and individuals; many organisations still report high numbers of cyber security breaches or attacks.

**90.** We build on the foundations of the previous strategy, evolve our approach and shift the dial on UK cyber resilience – placing particular emphasis on:

- scaling up our work to make the internet automatically safer, preventing attacks, building in basic protections to benefit all UK businesses, organisations and citizens, and increasing support available to those least able to protect themselves online
- setting an ambition for government to act as an exemplar of best practice in cyber security
- embedding cyber security as a core part of good business through better use of regulation and other incentives, and harnessing the power of our threat insight to build communities that can defend themselves
- underpinning all of this with objectively-measurable standards, evidence and data and moving from gathering to acting on that data

**91.** In this strategy the concept of cyber resilience has three key aspects. First, the nature of the **risk** needs to be understood. Second, we need action to **secure** systems to prevent and resist cyber attacks. Third, recognising some attacks will still happen, we need to prepare for these, to be **resilient** enough to minimise their impact and be able to recover.

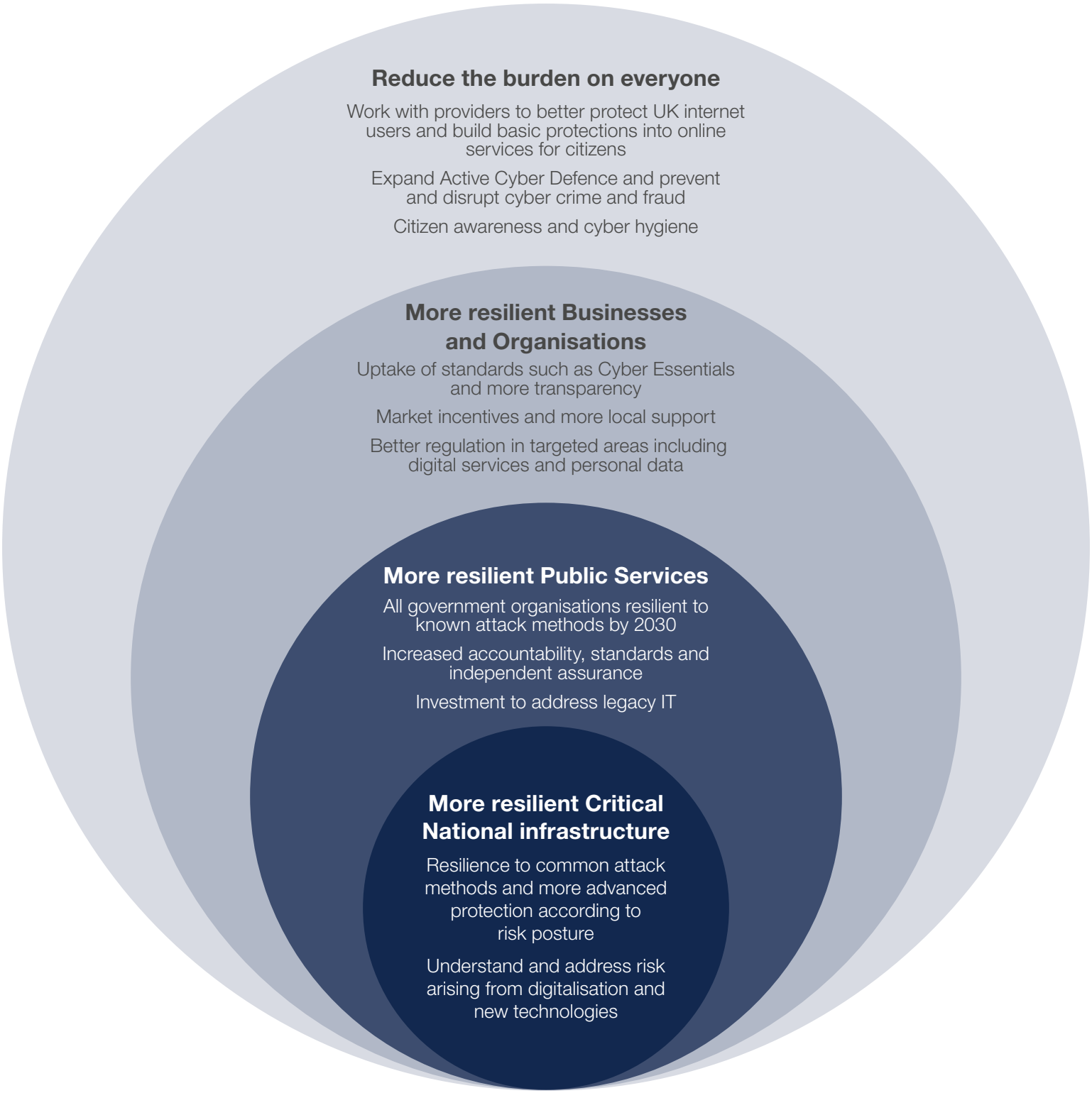
**92.** Our approach will be tailored to each audience, supported by national capabilities that enable us to address systemic risks. The audiences we seek to protect and influence are UK citizens, businesses and organisations, the government and public sector, and those who operate our critical national infrastructure (providing the key services such as drinking water, electricity, finance, transport and telecoms which we all rely on).

**93.** We will focus first on steps to secure the digital environment for all UK internet users, prevent attacks, build basic security in products and services, and help individuals and small businesses and organisations with basic actions to improve cyber security. As we move through to those with greater responsibility and capability to put in place additional layers of security and resilience proportionate to the risk, this will culminate in the highest level of protection expected for the key public and essential services our people and economy rely on.

**94.** This must be a shared endeavour between the government and all parts of the economy and society. It is the responsibility of boards of businesses and organisations to manage their own cyber risk. Our aim is to set clear expectations underpinned by the right framework of incentives, support and regulation to enable improvement and transfer the burden of cyber security risk away from end users and towards those best placed to manage it.

**95.** We require government departments, the wider public sector and regulated operators of critical national infrastructure (CNI), to raise their standards and manage their risk more proactively. We expect large businesses and organisations, including providers of digital services and platforms to be more accountable for protecting their systems, services and customers as a core part of running their business. In return, government will do more to secure the digital environment and tackle systemic risks and provide support through advice, tools, accreditation in the marketplace, and developing the skills that enable improvement.

**96.** Our efforts to promote cyber resilience in the UK must also form part of our international engagement. The deepening globalisation of supply chains, IT platforms, multinational businesses, and the internet itself, mean we cannot improve the UK's cyber security in isolation. To respond to this challenge we will need to continue building a better understanding of the linkages between UK and global cyber resilience, addressing areas of high risk and working with international partners to build resilience that facilitates digital transformation, security and trade, for mutual benefit as set out in the Pillar 4: Global Leadership chapter.


Reduce the burden on everyone
Work with providers to better protect UK internet users and build basic protections into online services for citizens
Expand Active Cyber Defence and prevent and disrupt cyber crime and fraud
Citizen awareness and cyber hygiene
More resilient Businesses and Organisations
Uptake of standards such as Cyber Essentials and more transparency
Market incentives and more local support
Better regulation in targeted areas including digital services and personal data
More resilient Public Services
All government organisations resilient to known attack methods by 2030
Increased accountability, standards and independent assurance
Investment to address legacy IT
More resilient Critical National infrastructure
Resilience to common attack methods and more advanced protection according to risk posture
Understand and address risk arising from digitalisation and new technologies

## Objective 1: Improve the understanding of cyber risk to drive more effective action on cyber security and resilience

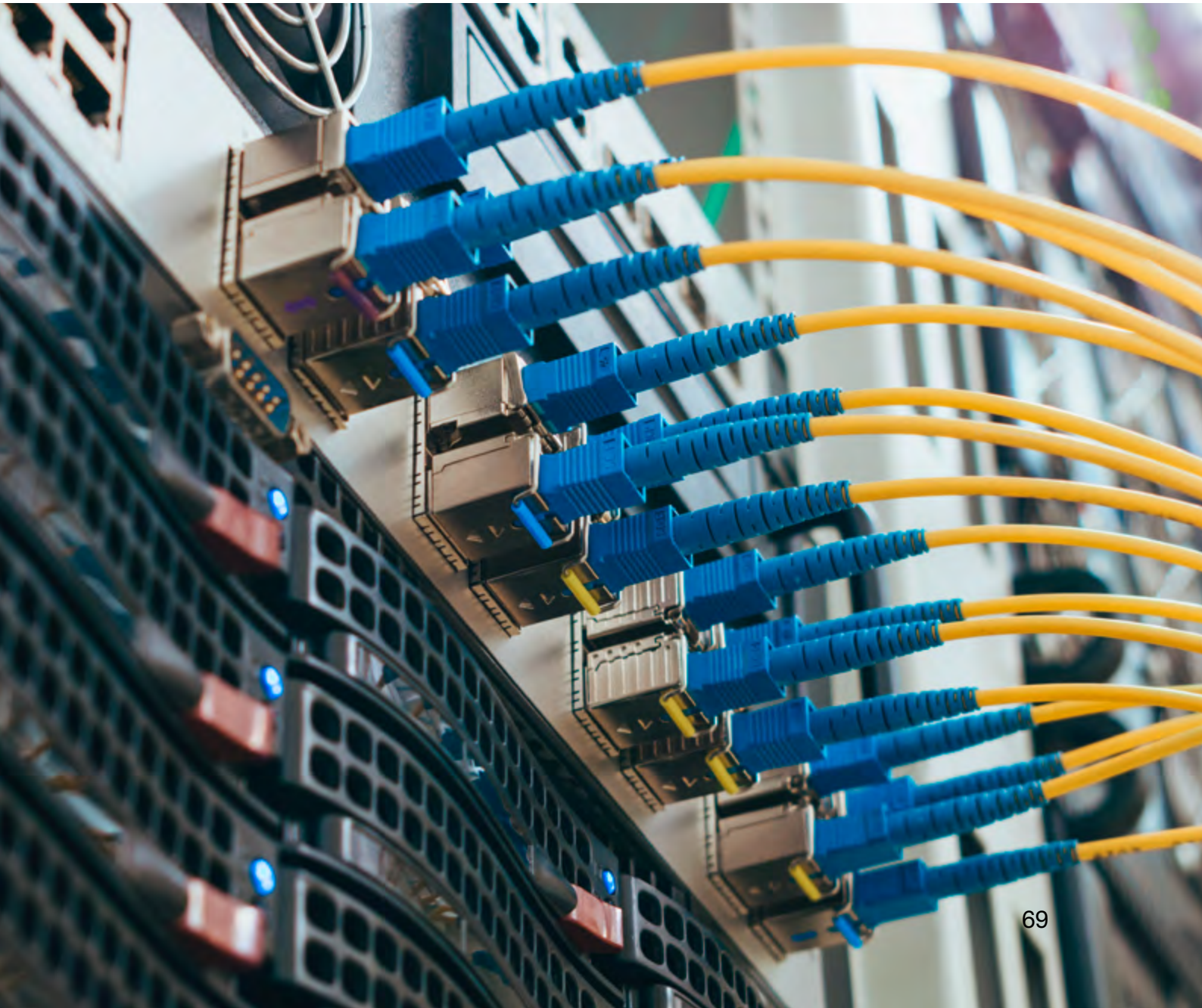
**97.** We will deliver a much closer partnership between government, businesses and organisations to drive up collective understanding of the risk, guide prioritisation and establish the case for action. We will support citizens by working with businesses and organisations that provide services to consumers; and further strengthen the government's ability to identify cross-cutting risks. We will achieve the following outcomes by 2025:

**98. Government has an up to date strategic understanding of the nation's cyber risk** and uses this understanding to identify systemic risk,communicate priorities and drive strategy and delivery. We will sustain and drive further value from significant investments made in 'understanding the threat' from the previous National Cyber Security Strategy; and build on existing efforts to understand risk in an increasingly interconnected world. This will include identifying where digital supply chains are too concentrated, and working with international partners to manage collective risks. We will also improve our recording of Computer Misuse Act (CMA) offences, understanding the links between data breaches and downstream criminality, and increasing our knowledge of how CMA offences are facilitating other types of criminal activity.

**99. Government is leading by example in its understanding of cyber risk.** We will adopt the NCSC's Cyber Assessment Framework (CAF) as the assurance framework for all government departments, and critical systems and common suppliers will be mapped. We will establish a new Government Cyber Coordination Centre (GCCC) and cross-Government Vulnerability Reporting Service (VRS) to enable the government to 'defend as one' when managing incidents, vulnerabilities and threats. The VRS will aim for valuable and trusted relationships with the security researcher community, delivering a reduction in vulnerabilities across the government estate. We will also continue to support and coordinate with similar initiatives in the devolved governments, such as the proposed establishment of a central coordination function for cyber resilience in Scotland.

**100. Across the UK's CNI, we will have a more sophisticated understanding of cyber risk**. We will increase the adoption of the Cyber Assessment Framework (CAF) or equivalents across CNI sectors, and improve comparability with other cyber security assessment and reporting frameworks in use. We will complete criticality reviews and map dependencies within CNI and its supply chains. We will build stronger partnerships with CNI owners and operators to improve access to threat and risk information, and agree risk posture. And we will work to understand new risks or where new CNI is emerging as a consequence of digitalisation and new technologies, including as part of broader priorities such as the transition to Net Zero.

**101. UK businesses and organisations have a better understanding of cyber risk and their responsibilities to manage them**. We will help organisations better understand the risk to their customers, including how the data they hold could be used to facilitate crimes like fraud, identity theft or extortion. And we will share more insights from research and data on the prevalence and impact of cyber attacks and relative progress sectors are making in improving cyber security.



## Objective 2: Prevent and resist cyber attacks more effectively by improving management of cyber risk within UK organisations, and providing greater protection to citizens

**102.** Our approach to preventing and resisting cyber attacks assumes: (i) that organisations have a responsibility to take action to manage their own cyber risk but stronger frameworks of accountability and good governance are needed at board level to make this a priority; (ii) that there is a role for government to play working with industry in taking steps to directly reduce risk at scale where it is uniquely placed to do so; and (iii) we must ensure support and guidance is available to help individuals, sole-traders and small businesses and organisations manage their cyber risk. We will achieve the following outcomes by 2025:

**103. Government has reduced harm to the UK at scale and reduced the burden on UK citizens**. We will increasingly act upstream on behalf of all internet users in the UK, expanding our Active Cyber Defence measures to support a wider range of sectors, including charities, academia and small-to-medium sized businesses and citizens. And we will strengthen protections to online services through increased engagement and information sharing with industry.

**104.** This work is complementary to other government priorities aimed at protecting UK citizens online, such as the draft Online Safety Bill and policy to counter economic crimes such as fraud.

**105.** It will mean working more closely with relevant sectors including online service providers, telecommunications, technology, banking and retail, to better protect UK internet users, including to: make it more difficult to register websites for illegal purposes, increase the take down and blocking of malicious content online, improve the recovery and return of stolen credentials, and enhance the security of UK telecommunications infrastructure. We will also develop options to give statutory backing to citizen protections should voluntary arrangements prove insufficient.

**106.** Our efforts to reduce harm at scale will also include tackling systemic risks from the digital supply chain. Where necessary we will intervene to promote supply chain diversification, as we are doing in telecommunications; we will strengthen our collective economic security with improved information-sharing and robust, predictable and proportionate approaches to foreign direct investment (FDI) screening in critical sectors, and establish clear requirements for critical and common suppliers to government.

**107. Government's critical functions are significantly hardened to cyber attack and all government organisations – across the whole public sector – will be resilient to known vulnerabilities and attack methods by 2030**. Our aim is to establish the UK's public sector as an exemplar of best practice. In support of this outcome we will publish the first dedicated Government Cyber Security Strategy. This will focus on more effective risk management processes, governance and accountability; centrally developed and employed capabilities (including Active Cyber Defence); more comprehensive monitoring of systems,

networks and services; rapid and scaled incident response; and investment in skills, knowledge and a culture that promotes sustainable change.

**108. Cyber risks to UK critical national infrastructure are more effectively managed**. Such services are by definition those that the country relies on most. We will continue to work closely with operators to achieve resilience against common attack methods as quickly as possible and to put in place more advanced protections where appropriate. For Operators of Essential Services designated under the NIS regulations this means at least meeting the baseline standard set by the relevant Competent Authorities for each sector.

**109.** In support of this outcome, we will review the government's ability to hold CNI operators to account to ensure they invest in the cyber security of critical systems and effectively manage their risk, including from their supply chains. We will strengthen the regulatory framework, to improve its coverage, powers, and agility to adapt, within the context of broader national security risk and rapidly changing threat and technology. This will start with a consultation on reforms to the NIS regulations, implementing the new security framework for UK telecommunications providers and developing a proportionate regulatory framework to ensure that the future smart and flexible energy system the UK requires to deliver Net Zero will be secure and resilient to cyber threats.

**110.** Alongside this we will: enhance the capability of regulators; invest in skills to improve CNI operators' ability to attract, develop, and retain cyber professionals (see UK Cyber Ecosystem chapter); and support operators' management of supply chain risk by stepping up engagement with critical suppliers and exploring the full range of levers, from guidance to legislative and procurement related proposals.

**111. The infrastructure on which our data use relies is secure and resilient**. This infrastructure is a vital national asset – one that supports our economy, delivers public services and drives growth. We will take a greater role in ensuring that data is sufficiently protected when processed, in transit, or stored at scale, for example in external data centres. We will build a stronger risk management framework to ensure higher security and resilience standards across the sector and implement the provisions in the National Security and Investment Act 2021 to strengthen investment screening. We will strengthen our work with international partners to ensure that increased global data access and flows do not increase the security risks facing the UK, and also address the security challenges posed by mass data collection.

**112.** We will also consider the increasing criticality of UK data infrastructure services in underpinning the economy and its role within critical national infrastructure. These measures are in line with the commitments set out in the National Data Strategy and the Integrated Review.

**113. A greater number of UK businesses and organisations are proactively managing their cyber risks and taking action to improve their cyber resilience.** We will provide support and drive behaviour change through the development of market incentives that encourage effective cyber security. Where necessary this will be complemented by targeted legislation to ensure that cyber risk is managed effectively by those who have the greatest responsibility to do so, and that the UK's cyber security legislation remains effective in the light of evolving risk and technologies.

**114.** In support of these aims, we will increasingly work with market influencers (procurers, financial institutions, investors, auditors and insurers) to incentivise good cyber security practices across the economy. We will propose improvements to corporate reporting of resilience to risks, including cyber risks. This will give investors and shareholders better insight into how companies are managing and mitigating material risks to their business. And we will continue to promote take-up of accreditations and standards such as the Cyber Essentials certification scheme and promote board level engagement in cyber risk management.

**115.** Targeted legislation will primarily focus around sectors where the potential impact of a cyber attack is greatest, including providers of certain essential and digital services, data protection in the wider economy, and for larger businesses. This will be complementary to the Plan for Digital Regulation, initially focussing on regulations governing the security of Network and Information Systems (NIS) – as outlined above and in the Technology chapter and the next steps for reforming the UK's regime for the protection of personal data.

**116.** Further detail outlining the action we will take to improve business resilience and cyber security across UK businesses and organisations will be set out in the Cyber Security Regulation and Incentives Review.

**117. Technical advice, self-help tools and assured products and services to improve cyber resilience are easy to find and continually improving, with a particular emphasis on helping citizens, sole-traders and small organisations**. We will continue to develop technically accurate, timely and actionable guidance and self-help tools through the NCSC. We will ensure messages are consistent, clear and provided through the most effective channels, whether via the Cyber Aware campaign, NCSC website, government, law enforcement networks or partnerships with industry; and we will make more support available at a local level. Through the 'Digital Entitlement', we will continue to fully fund Essential Digital Skills qualifications for adults who need them, ensuring learners have the basic digital skills they need to be safe and responsible online. And we will help businesses and organisations navigate the complex cyber security market, extending our frameworks for assured products and services, and developing commercial offerings around Cyber Essentials which will make it easier for small businesses to access basic advice.

## Elis Power, Cyber Protect and Prevent Officer, Tarian Regional Cyber Crime Unit

Tarian Regional Cyber Crime Unit is a multidisciplinary team of police officers and staff seconded from the Welsh Police forces. Their mission is to contribute towards the provision of a safer and more secure cyber-environment in Southern Wales.

Cyber Protect/Prevent Officer Elis Power works for the engagement team:

"It's a cliché but there is no such thing as a typical day on the unit. From day to day, I could be responsible for delivering presentations containing advice for internal police departments, or external organisations, to ensure that they have a solid understanding of how to protect themselves and their workplace against cyber threats. I could also be presenting to young people in schools on topics ranging from internet safety through to the Computer Misuse Act 1990. I frequently attend meetings with partner agencies and forces to discuss new threats and associated guidance for our audiences. I also engage with organisations from which we've received vulnerability alerts, take part in national operations, guest appear at relevant events and conferences, and find time to continually upskill my abilities and knowledge base".

## Objective 3: Strengthen resilience at national and organisational level to prepare for, respond to and recover from cyber attacks

**118.** Despite efforts to understand the risk and take preventative actions some incidents will still occur. We need to strengthen capabilities for incident management and response across all organisations, to minimise the harm caused and provide better support to victims. We will achieve the following outcomes by 2025:

**119. The UK's strategic management and coordination of the response to nationally significant cyber incidents is even more effective.** We will build upon the government's experience of responding to significant cyber incidents, ensuring that lessons identified are used to improve our policies and processes. We will share crisis management experience with international partners and industry and, in turn, identify best practice from elsewhere to enhance our preparedness and processes. We will ensure that NCSC and law enforcement incident management teams have the requisite expertise and tools to respond to the full range of evolving incident types and co-ordinate a national response to priority threats.

**120. It is easier to report cyber incidents and victims of cyber crime receive better support**. Reporting information will also be used to help prevent future incidents and support law enforcement to investigate, disrupt, and prosecute cyber criminals. In support of this we will deliver a new national fraud and cyber crime reporting and analysis service to replace Action Fraud by 2025. We will encourage more reporting of cyber incidents in other ways, including through a new business reporting capability in the City of London Police. In regulated sectors we will enable regulators to require reporting of a broader range of incidents including 'near misses'. The roll out of the National Economic Crime Victim Care Unit will improve the support and guidance available to victims after what can be a stressful and harmful experience.

**121. Government and CNI are more prepared to respond to and recover from incidents, including through better incident planning and regular exercising.** We will help UK government and CNI operators find the cyber exercising and incident management services they need from the marketplace by expanding the NCSC's accredited scheme for Cyber Incident Response and introducing a new scheme for exercising.

**122.** Within government, monitoring and detection capabilities will be improved within departments and across the government digital estate. We will ensure lessons are identified and used to improve our policies and processes; share crisis management experience with international partners and industry; and ensure that our incident management teams have the requisite expertise, capacity and capabilities to respond to the full range of evolving incident types.

**123.** Within CNI we will set out clear requirements for exercising and testing or adversary simulation across CNI operators, and stimulate innovation and collaboration in incident response and exercising, considering application of models such as the Financial Sector Cyber Collaboration Centre. And as part of our ambitions on technology (outlined in the next chapter) we will establish a national laboratory for operational technology security as a centre of excellence for testing, exercising and training on critical industrial technologies to build capability in this area, in collaboration with industry, academia and international partners.

**124. UK businesses and organisations have a clearer understanding of what to do in the event of an incident, who to call, who can help and how to recover**. We will improve access to training and exercising, supported by assured industry services, including a new Cyber Incident Response scheme and Cyber Incident Exercising service. We will ensure access to consistent nationwide law enforcement support for individual victims of cyber crime and encourage small businesses and organisations to take advantage of local support, such as their regional Cyber Resilience Centre.

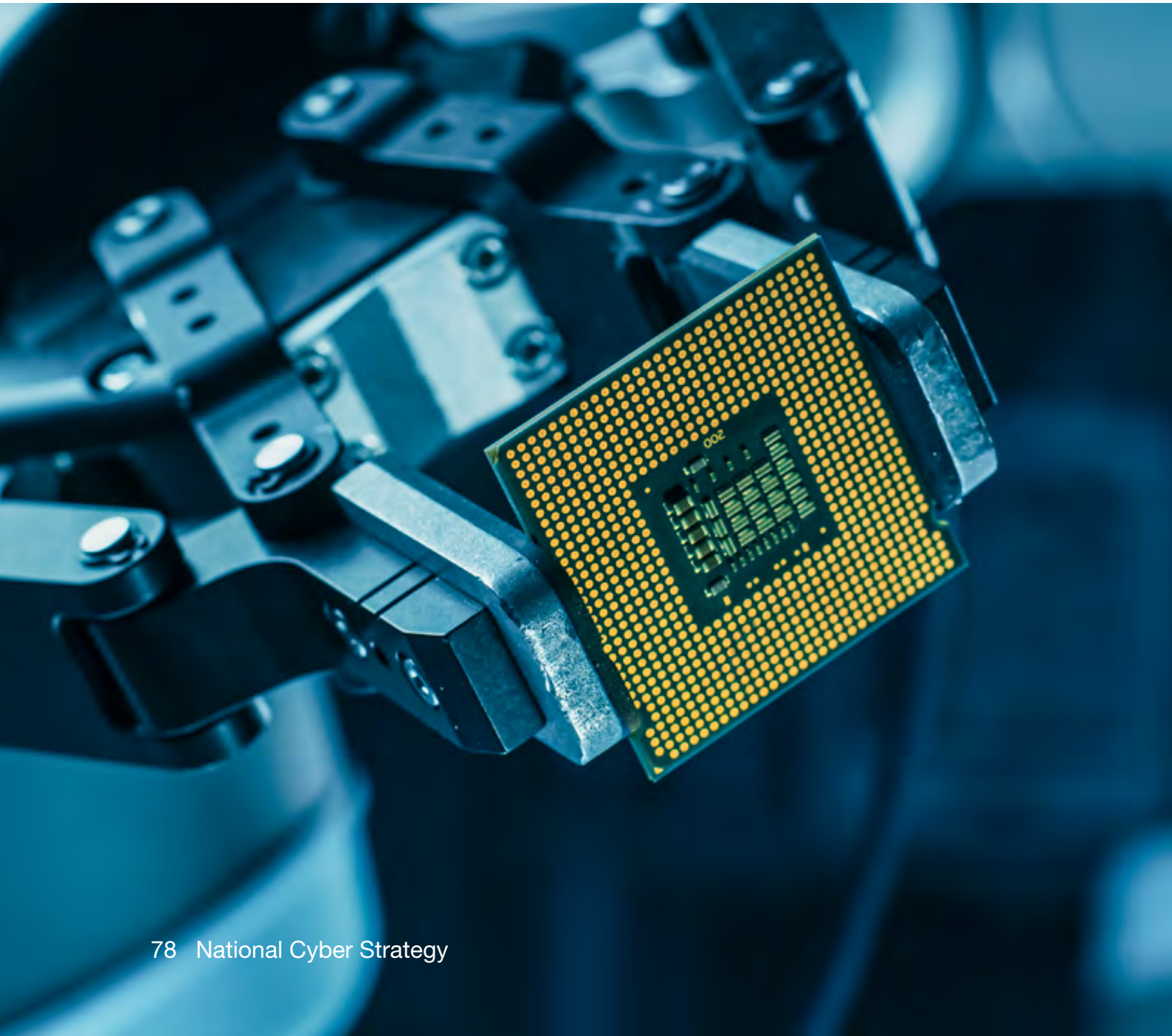
### Daniel Ng, CEO, CyberOwl

CyberOwl benefited from the government's cyber development programme. We provide cyber security monitoring and analytics for operational assets in the maritime and CNI sectors. The drive towards sustainability demands more connectivity and digitalisation of field assets, exposing them to cyber risks. CyberOwl helps operators identify and map their assets, gain early warning of cyber risks and prove to themselves and regulators that they have secured it. We work with the world's largest maritime asset operators across EMEA and Asia Pacific to improve resilience of the global shipping logistics supply chain. In 2021, we have grown bookings by 14 times and doubled operations in the UK and Singapore.

## Jen Ellis, Vice President of Community and Public Affairs, Rapid7

My work involves talking to security professionals and leaders in organisations of all sizes and sectors to understand the challenges they face and try to identify solutions to help them advance their cyber security. I consistently hear that organisations are overwhelmed and don't know where to focus, how to get started, or how to make progress. It can also be hard for technical staff to get buy-in from leadership. Having a clear, consistent, transparent cyber strategy from the government can help address this. It gives technical staff something to point to as part of their discussions with leadership. It also identifies core areas of focus and a potential path towards maturity. Cyber security is still hugely complex and never ending, but with the widespread cyber strategy there is a greater understanding of its importance and a feeling that we are all in this together.

# Pillar 3:
# Technology Advantage



# Taking the lead in the technologies vital to cyber power

**125.** Some technologies will be critical in shaping the future of cyberspace. Countries that are able to establish a leading role in these technologies will be better positioned to influence the way that they are designed and deployed, more able to protect their security and economic advantage, and quicker to exploit opportunities for breakthroughs in cyber capabilities. As technology becomes an increasingly important tool of geopolitical power, competition in this arena will intensify.

**126.** For the UK, pursuing strategic advantage through science and technology, and the data access it depends on, will be a precondition for achieving our wider goals as a cyber power. The government has taken steps in previous strategies to stimulate research and innovation in cyber security technologies, such as through accelerator programmes for start-ups and the Academic Centres of Excellence in Cyber Security Research, and to encourage the development of consumer devices that are 'secure by design'. However, we now need a more ambitious and proactive approach to maintain a stake in critical technologies and avoid becoming overly dependent on competitors and adversaries.

**127.** The Integrated Review set out plans to make the UK a Science and Tech Superpower and use science and technology to build and sustain our strategic advantage. This strategy supports the work of the National Science and Technology Council and the Office of Science and Technology Strategy in pursuing that goal, as well as complementing the UK's strategies in areas such as Artificial Intelligence, Quantum Technologies and Data.

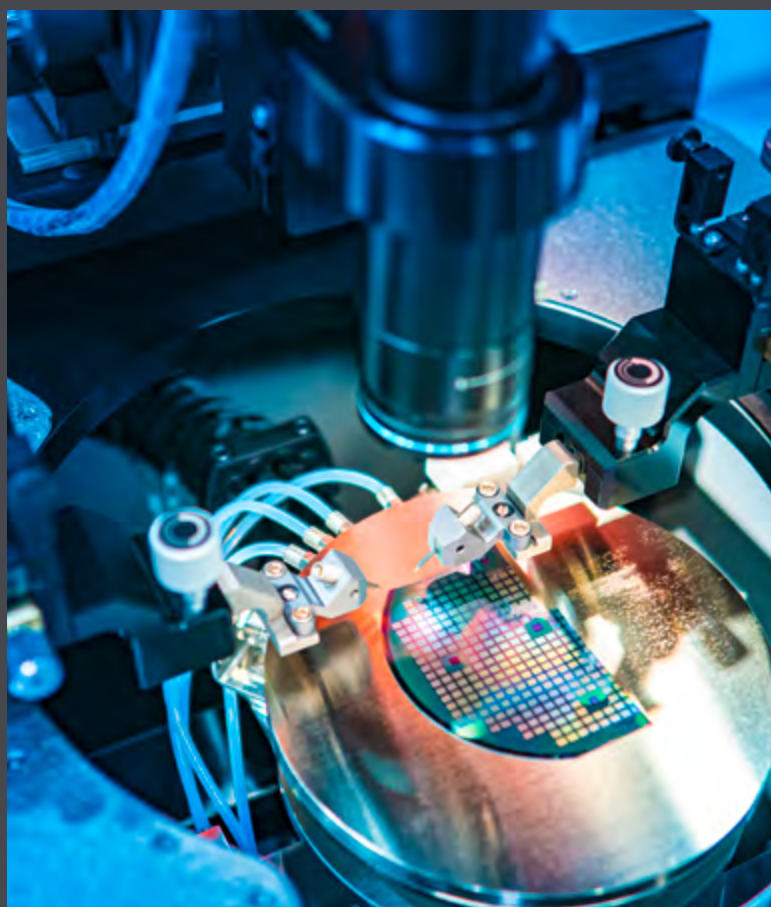
**128.** We will strengthen our ability, led by the technical expertise of the National Cyber Security Centre (NCSC) and others across government, to identify the areas of technology most critical to our cyber power. We will take national-level strategic decisions about priorities, working within the Own-Collaborate-Access framework set out in the Integrated Review. In select areas we will invest in the research and development activity and strategic partnerships needed to develop the UK's domestic capabilities, and where we rely on global markets we will work with industry, regulators and international partners to encourage trustworthy and diverse supply chains, and to shape standards to ensure technologies are secure and open. We will also strengthen the UK's ability to exploit and protect the growing quantities of data and information generated by and driving innovation in emerging technologies, building on the framework set out in the National Data Strategy to maximise the benefits for our economy and society.

# Technologies vital to Cyber Power

A variety of existing and emerging technologies will be critical to the UK's cyber power and we need to be able to anticipate, assess, and act on these developments. We expect to prioritise a range of technologies and applications as we deliver the strategy, such as those set out below. This is not intended as an exhaustive or static list and our priorities will continue to evolve in consultation with industry, academia and technical experts:

- 5G and 6G technology, and other emerging forms of data transmission
- Artificial intelligence (AI), including the need to secure AI systems and the potential for the use of AI to enhance cyber security in a wide array of applications such as network monitoring
- Blockchain technology and its applications such as cryptocurrencies and decentralised finance
- Semiconductors, microprocessor chips, microprocessor architecture, and their supply chain, design, and manufacturing process
- Cryptographic authentication including for identity and access management and high assurance cryptographic products
- Internet of Things and technologies used in consumer, enterprise, industrial and physical environments such as connected places
- Quantum technologies, including quantum computing, quantum sensing and post-quantum cryptography

This work will support, and be aligned to, the delivery of a number of strategies and outcomes across government, for example, the National Data Strategy, the National AI Strategy and the Integrated Review, as well as the technology focussed outcomes within this Pillar.



## Objective 1: Improve our ability to anticipate, assess and act on the science and technology developments most vital to our cyber power

**129.** To build and sustain a competitive edge in cyber-related technologies we need a coordinated, rigorous and consistent approach to identify and analyse critical areas of science and technology and prioritise national effort. This will require us to develop our research and technical expertise within government and academia even further. We will integrate this with new government structures for science and technology horizon-scanning and intelligence whilst drawing on the insights of industry experts and leveraging our overseas network to understand the priorities and systems of international partners and competitors. We will achieve the following outcomes by 2025:

**130. Government is better able to analyse new and developing science and technology and understand the implications for UK cyber policy and strategy**. We will expand our research capabilities including the NCSC's new applied research hub in Manchester, with a focus on emerging technology in areas such as connected places and transport, working alongside experts in the Government Office for Science and elsewhere. We will draw on expertise from outside government, supporting the four Cyber Security Research Institutes and nineteen Academic Centres of Excellence in Cyber Security Research, funding Pathfinder Awards for researchers in priority subjects, and leveraging our overseas footprint and international partnerships more effectively.

**131. This improved understanding is more quickly and effectively informing the government's wider horizon-scanning, prioritisation and decision-making**, allowing us to take a more proactive approach to exploit opportunities and mitigate risks. We will establish a new internal horizon-scanning function to anticipate science and technology advancements and their cyber implications. We will take more informed decisions to prioritise key cyber technologies, directing R&D and policy development that will advantage UK security. Where appropriate, this will inform wider decision-making on science and technology priorities through the Office for Science and Technology Strategy and National Science and Technology Council.

**Máire O'Neill, Principal Investigator at the Centre for Secure Information Technologies (CSIT)**

CSIT is one of the UK's largest cyber security focused university technology research centres. Led by Principal Investigator Professor Máire O'Neill, it was as a result of being selected as one of the country's first Innovation & Knowledge Centres in 2009. CSIT's successful research, innovation and industry engagement have led to the significant growth of its reputation both nationally and internationally over the past decade. CSIT has been a critical factor in the success of the Northern Ireland Cyber Security Cluster through its support of spinout activity, indigenous business scale-up and FDI in the region. From a standing start in 2009 Northern Ireland's cyber sector now employs 2,300 people across 104 companies, generating £110 million in salaries each year.

## Objective 2: Foster and sustain sovereign and allied advantage in the security of technologies critical to cyberspace

**132.** Where the UK has the potential to establish a leading position or secure a competitive advantage in key areas of cyber technology, or where reliance on non-allied sources of supply poses unacceptable security risks, we will seek to develop our domestic industrial base. There will be some areas where we need to maintain a truly sovereign capability, and others where we will collaborate with international partners or seek a leading position in one aspect of the market. This will require a coordinated approach to stimulating innovation and R&D in collaboration with industry and academia. We will achieve the following outcomes by 2025:

**133. The UK is more successful at translating research into innovation and new companies in the areas of technology most vital to our cyber power.** We will support academics across the UK to commercialise and operationalise their research by adopting a more challenge-based approach in collaboration with industry partners. This will identify ideas with the highest potential and stimulate investment from funders. And we will build on the approach set out in the Innovation Strategy, supporting the development of more established ecosystems around key technologies, ensuring that the UK's advantage is more robust and difficult to copy.

**134. The UK is in an even stronger position as a world leader in secure microprocessor design**.[26] We will build on the Digital Security by Design programme that has developed a new, more secure technology for computer chips to protect software from vulnerabilities. We will bring this experience to bear on Artificial Intelligence processors to give UK vendors an international advantage. And we will work with the National Quantum Technologies Programme to design a security model for quantum computers and to ensure that UK companies are world leading in this technology.

**135. The UK is regarded as a world leader in research into the security of operational technologies and critical industrial control systems, and in our ability to test and exercise them in the UK**. We will establish a national laboratory for operational technology security in partnership with industry and academia. It will host world leading research programmes and provide government, military, industry and international partners with the facilities for exercising and testing these technologies here in the UK. And as confirmed in the 5G Telecoms Supply Chain Diversification Strategy, we will establish the UK Telecoms Lab, bringing together the government and the regulator with industry to support the new telecoms security framework and help to increase the diversity of telecoms equipment vendors in the UK's supply chain.[27]

**136. The government is better able to protect UK innovation and intellectual property in critical cyber technologies against hostile activity**, sustaining our competitive edge.[28] We will invest in the resources and expertise we need to provide technical leadership on the security of these technologies as they develop, including advising on foreign direct investment risks in line with the goals of the National Security and Investment Act 2021. And we will continue to work with businesses and academia to create a trusted environment in key areas of research and development, and develop robust measures to prevent the theft of data and intellectual property.

[26] Microprocessors are the brains of many of the devices we use today. They are ubiquitous, including in critical areas such as telecoms, defence, healthcare and across our major industries. Technological advances in systems design are currently held back by security and safety concerns, which are magnified by increasing system complexity.

[27] DCMS, 5G Supply Chain Diversification Strategy (2020)

[28] With a particular focus on those sectors identified in the National Security and Investment Act 2021: advanced robotics, artificial intelligence, communications, computing hardware, cryptographic authentication, and quantum technologies

# Digital Security by Design

Seventy per cent of current cyber security vulnerabilities exploit a flaw in how microprocessors are designed that has been known about since the 1970s. These microprocessors are found in every digital device from televisions to telecoms. The government has been working with the tech sector to fix this and by 2025 a new microprocessor design will be available for smartphones, and a growing list of other devices.

Changing the design of microprocessors requires global partnerships and investment. With UK leadership, and £70 million of investment from the government, security is being designed into future devices, hugely reducing the risk of a successful cyber attack.

This game changing technology was researched and developed in the UK. Tech leaders including Microsoft, Google and others are investing to bring these new security benefits to their products. Researchers in universities across the UK are working to find new ways to use this secure technology better and the government is supporting UK SMEs to find new markets for products that have this new security built in.

**Phil Wilson, Director, Research & Development at The Hut Group**

The Hut Group is an e-commerce business focused on fast moving consumer goods. We have over 200 websites running on a common platform with up to 3000 orders per minute to process so the security of our platform and our customers is a top priority. We invest huge amounts of effort to ensure that any cyber attack can be contained and that is why we are so excited by the possibility of using Digital Security by Design (DSbD) tech in our systems. Running our systems on these new microprocessors, developed in a £180 million government-industry partnership, would make our systems more resilient but managing that transition is complex as we cannot adopt new tech unless it meets our performance requirements. It has been a privilege to be the first demonstrator project for the DSbD programme and we hope to benefit from this new security across all our systems in the near future.

## Objective 2a: Preserve a robust and resilient national Crypt-Key enterprise which meets the needs of HMG customers, our partners and allies, and has appropriately mitigated our most significant risks including the threat from our most capable of adversaries

**137.** Crypt-Key is the term used to describe the UK's use of cryptography to protect the critical information and services on which the UK government, military and national security community rely, including from attack by our most capable adversaries. It underpins our ability to choose how we deploy our national security and defence capabilities. To be a world-leading Crypt-Key nation we need the right skills and technologies both in government and in the private sector.

**138.** We will continue to invest in our capabilities in government and work with our domestic Crypt-Key industry to ensure the UK remains one of a handful of nations able to develop sovereign Crypt-Key into the future. We will also continue to provide global leadership in Crypt-Key, including supporting NATO as a supplier of key material. This leadership will bring second order benefits in sustaining a highly skilled industry in the UK and preserving our strength in highly resilient engineering, with the potential to enable new robust capabilities for other high assurance contexts such as critical national infrastructure. We will achieve the following outcomes by 2025:

**139. A more resilient and secure UK Crypt-Key enterprise with a more sustainable, world-leading industrial base**, supplying the full range of solutions that the UK needs and exporting to chosen partners and allies. We will combine the capabilities and expertise of government and industry more effectively, and take a more rigorous, national approach to managing the enterprise. This will ensure that we grow the distinct, specialist skills that we need.

**140. The UK has stronger Crypt-Key capabilities and services in government**, able to meet the evolving needs of the UK and our allies and ensuring we remain at the forefront of Crypt-Key development. We will provide strong technical leadership to understand user requirements and improve our core services, including provision of key material and assurance of products and systems. We will also transform Crypt-Key services, harnessing new technologies so that they become more flexible and invisible.

**141. The UK has advanced its global leadership in Crypt-Key and increased exports to our partners and allies**. We will maintain our leadership role in the Five Eyes, NATO and other international partnerships and shape the development of internationally recognised standards to enable UK Crypt-Key solutions to be interoperable. And we will work with the industry to maximise export opportunities.

## Objective 3: Secure the next generation of connected technologies, mitigating the cyber security risks of dependence on global markets and ensuring UK users have access to trustworthy and diverse supply

**142.** Over the next decade we will continue to see computing power, internet connectivity and automation embedded into more and more parts of our environment, including physical objects and infrastructure and, in the longer-term, humans themselves. This will extend the scope of cyberspace and vastly increase the volume of data generated. The ability to manage data safely and securely will become ever more critical to the secure running of our economy.

**143.** We need to ensure that wherever possible the next generation of connected technologies are designed, developed and deployed with security and resilience in mind and as part of a concerted effort to embrace a 'secure by design' approach. The global nature of technology supply chains means we will need to use all our available levers to more actively manage the risks of technological dependence. Where possible we will seek to ensure that security is built in; where we cannot do this, we will implement robust measures to mitigate risk, including domestic regulation and international collaboration on standards. We will achieve the following outcomes by 2025:

**144. Consumer connectable products sold across the UK meet essential cyber security standards**. We will introduce and implement the Product Security and Telecommunications Infrastructure Bill to enable enforcement of minimum security standards in all new consumer connectable products sold in the UK. We will support a cyber secure transition to a smart and flexible energy system, including smart electric vehicle charge-points and energy smart appliances. We will work with standards bodies, industry and international partners to influence the global consensus on technical standards. And we will help UK organisations to procure, deploy and manage connected devices in a more secure way, including by means of new security guidance for enterprise connected devices.

**145. Major providers of digital services, including cloud, software, managed services and app stores, are required to follow better standards of cyber security**, helping to protect organisations and consumers from cyber threats. We will strengthen and expand the existing regulation of digital service providers and boost the capability of the ICO to ensure digital providers are managing the risks associated with their services more proactively. We will continue to engage with industry, including the major technology companies, to harness market expertise and ensure that everyone plays a role in securing the UK's digital supply chains. And we will lead the development of international policy solutions that focus on digital suppliers.

**146. The UK is at the forefront of the secure and sustainable adoption of connected places technology** for the benefit of citizens and businesses. Connected places, sometimes known as smart cities, have the potential to provide tangible benefits to society: managing traffic, reducing pollution, and saving money and resources. However, the interconnectivity that allows places to function more efficiently also creates cyber vulnerabilities and the potential for cyber attacks. We will build on the NCSC's security principles for connected places to reduce the risks posed to businesses, infrastructure, the public sector and citizens.[29] We will strengthen the capability of local authorities and organisations such as ports, universities and hospitals, to buy and use connected places technology securely. And we will build an international consensus for a consistent and effective approach to the security of connected places.

**147. Cyber security is designed into other emerging technologies deployed in the UK**. We will identify novel and emerging technology applications that have the potential to create cyber security risks, and ensure the UK is at the forefront of the safe and secure development of these technologies. As the government considers options for a UK capability in digital twin and wider 'cyber-physical infrastructure' technology, we will ensure that cyber security is at the heart of decision-making.[30] And we will roll out an assurance scheme to ensure that the UK is in a strong position for a wide range of connected and automated vehicle deployments.[31]

[29] NCSC, Connected Places Cyber Security Principles (2021)
[30] Announced in the Innovation Strategy (2021)
[31] The Connected and Automated Vehicles Process for Assuring Safety and Security (CAVPASS)

## Shadi A. Razak, CTO and co-founder of Angoka

The publication of secure connected places guidance by the government and the increasing use of autonomous vehicles highlights the importance of security in our society. Angoka is a proud alumni of the NCSC Cyber Accelerator programme. We provide solutions for a wide range of applications, from critical national infrastructure to land and air mobility and more, ensuring end-to-end resilience and security assurance.

The company mission is to ensure the safety and resilience of Smart Cities and mobility, which are becoming more complex and reliant on networks of connected devices and machine-to-machine communication. Our solution allows the creation of trusted zones operating a decentralised, quantum-proof security, dynamically updated to always provide a moving target for attackers. It means device owners can take full control of their security.


Angoka Team demonstrating their solution

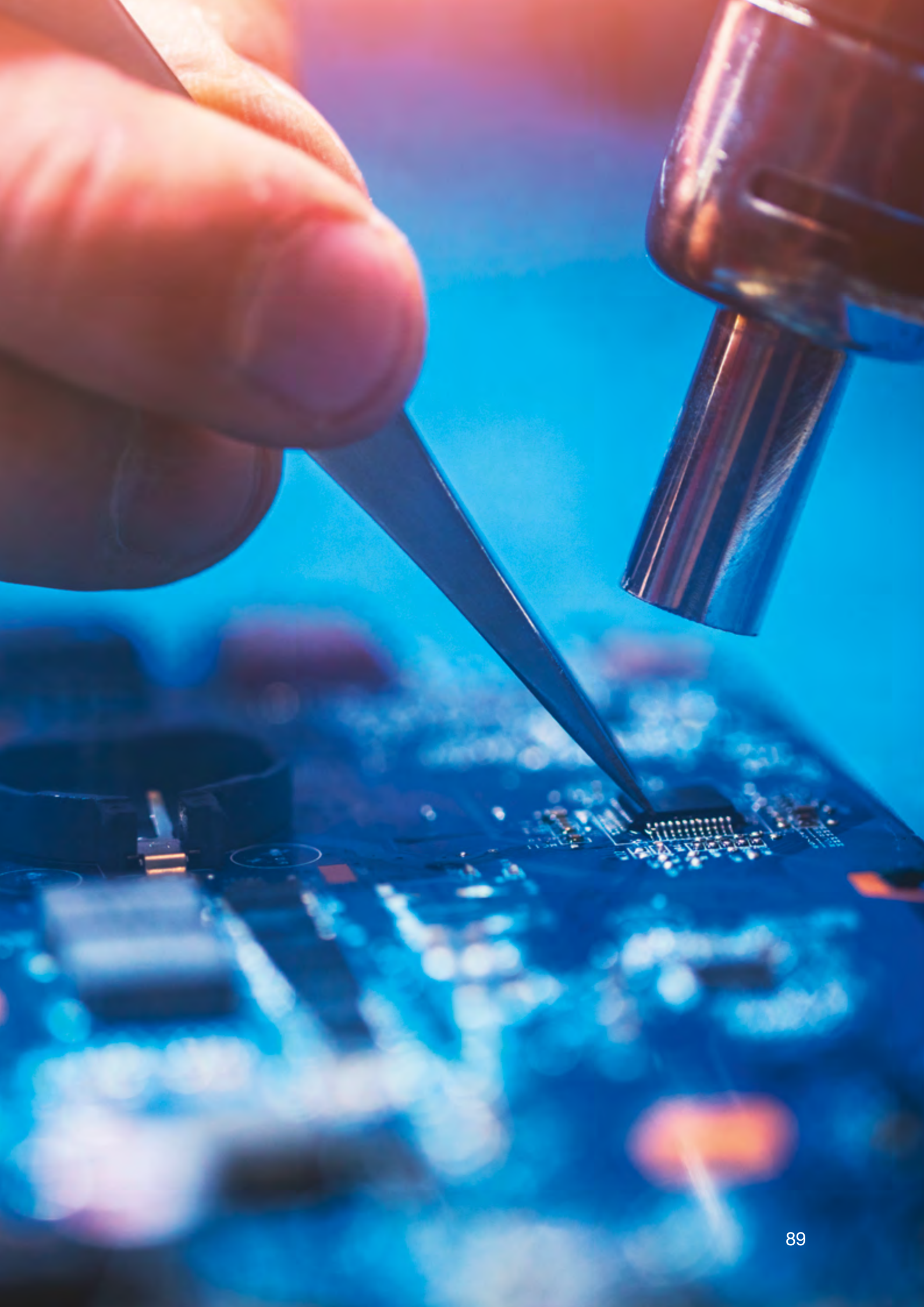
## Objective 4: Work with the multistakeholder community to shape the development of global digital technical standards in the priority areas that matter most for upholding our democratic values, ensuring our cyber security, and advancing UK strategic interests through science and technology

**148.** Global digital technical standards are a core part of the functioning of the internet, telecommunication networks, and emerging technologies. How they are developed and deployed can impact our cyber security objectives, economic prosperity, and our norms and values. Historically these standards have been shaped by those with the most market power and there are material barriers to entry that prevent some important stakeholders, including SMEs, academics, and other experts, from participating. We will achieve the following outcomes by 2025:

**149. More engaged multistakeholder participation in the global digital technical standards ecosystem.** We will reinforce multistakeholder participation in key standards development organisations and lead by example with our delegations to the International Telecommunication Union. We will promote open discussions on the key trends and considerations for policy makers through the UN Internet Governance Forum and other forums. And we will strengthen coordination and information sharing with international partners, including through the Digital Standards Points of Contact Group, set up during the UK's G7 presidency.

**150. Global digital technical standards in priority areas for the UK that are shaped more effectively by democratic values, cyber security considerations and UK research and innovation in emerging technologies**. We will work with industry, academia, technical experts and civil society in areas such as internet protocols, future networks and Artificial Intelligence (AI), to raise awareness of important public policy considerations in technical standards development. We will pilot an AI standards hub to support the UK's global engagement in AI standardisation, as set out in the National AI strategy.

**151.** All of this will be supported by strategic coordination mechanisms within the UK, such as the initiative set out in the National AI Strategy between the government, the British Standards Institution (BSI) and the National Physical Laboratory. This engagement will also support UK prosperity by promoting standards that enable innovation and facilitate growth and levelling up.



# Pillar 4:
# Global Leadership

# Advancing UK global leadership and influence for a secure and prosperous international order

**152.** A free, open, peaceful and secure cyberspace remains critical to our collective security and prosperity, and international engagement will continue to be vital for delivering all UK cyber strategy objectives. However, to respond to an era of systemic competition, the UK will now take a more activist international leadership role to promote our interests and values in cyberspace. UK activity in cyberspace and our cyber expertise will also be placed at the heart of delivering the government's broader foreign policy agenda: we will use them proactively to help achieve an open, secure and prosperous international order.

**153.** We will reinforce our core alliances, whilst working with a wider range of partners, including industry, global technical standards bodies, civil society and academia as a problem-solving, burden-sharing nation. We will invest in deeper relationships with partners in Africa and the Indo-Pacific and seize opportunities for new, more agile alliances. We will also continue to enhance our diplomatic toolkit, connecting our overseas influence to our domestic strengths, leveraging our operational and strategic communications expertise, skills programmes and economic partnerships as a global force for good. Our approach is in the interests of global security and prosperity, not just our own.

## Objective 1: Strengthen the cyber security and resilience of international partners and increase collective action to disrupt and deter adversaries

**154.** Collective action and mutual resilience are critical to countering threats upstream, whilst also reducing the incentives for cyber threat actors to carry out attacks against the UK and its partners. We will achieve the following by 2025:

**155. The UK's international partners have stronger capabilities, political resolve, governance, and systems for investigating and disrupting cyber threats, as well as for building resilience**. This will have resulted in a reduced threat from abroad to UK citizens. We will prioritise our cyber capacity building assistance in Eastern Europe, Africa and the Indo-Pacific, and continue to work with key allies in the Middle East and the Americas. We will develop a more integrated, whole-of-government technical offer, with greater investment in law enforcement and defence expertise, drawing more on UK industry and academia. Our focus will be on protecting critical international supply chains and infrastructure, advancing the secure use of digital technologies and working with industry partners to do so at scale.

**156.** We will also do more to build the capacity of civil society organisations, enabling a values-driven debate around technology and society and building local mechanisms of accountability. And we will continue to work with effective multilateral organisations and partnerships including the United Nations, Five Eyes, NATO, G7, European Union, Commonwealth, OECD, Global Forum on Cyber Expertise (GFCE), ASEAN Forum, African Union and the World Bank.

**157.** To improve our protection of UK interests and citizens overseas we will also develop and deliver an international cyber hygiene campaign for UK overseas missions that will be tailored and delivered locally. The aim will be to raise the cost of malicious activity, such as hacking, data and IP theft and ransomware. The campaign will be delivered through our diplomats, country-based staff, the local British business community and implementers of UK development programmes.

**158. A broader international alliance that is willing and able to impose more meaningful consequences on the UK's adversaries**. We will improve international resolve and capabilities through greater diplomatic engagement, operational collaboration, information sharing and joint exercising. By working through policy, operational and law enforcement channels we will increase the impact of measures, such as targeted cyber sanctions, as well as identify new tools for raising the costs for cyber threat actors. We will build more mutual understanding across key allied and partner countries' cyber forces and better integrate cyber operations into allied operations across all domains: land, sea, air, space and cyberspace.

**159.** And we will continue to support the development of the NATO alliance's cyber security capabilities for strengthened collective action, including supporting the processes to integrate sovereign cyber effects provided voluntarily by the UK and some other allies, into NATO operations and missions.

## Objective 2: Shape global governance to promote a free, open, peaceful and secure cyberspace

**160.** States who do not share the UK's values exploit the challenges presented by a free and open internet to push forward their authoritarian visions for cyberspace, under the guise of security. The UK will take a more proactive approach, working with our allies and partners to ensure international rules and frameworks develop in line with our democratic values. We aim to support national and global economic growth, enhance collective security, encourage responsible use of offensive cyber tools and enable real consequences for malicious and irresponsible activities. We will achieve the following outcomes by 2025:

**161. Global governance of cyberspace and the internet is protecting UK interests and values, with the UK and our partners having greater influence** over the development and implementation of international governance and standards frameworks. We will take a more progressive and proactive approach to shaping the frameworks that govern cyberspace to promote global economic growth and security. We will design and deliver practical steps that unblock the international debate on the application of rules, norms and principles in cyberspace and move it towards a consensus on effective constraints on destructive and destabilising activity. We will do this through key regional and specialist organisations including the OSCE, ASEAN and the GFCE and engage constructively with the UN process to develop a new international cyber crime treaty which sits alongside the Budapest Convention, ensuring that it strengthens international cooperation and maintains human rights protections.

**162.** We will also continue to promote the Budapest Convention on cyber crime, working with international partners to make a compelling case for it to remain the premier international agreement for cooperation. And we will continue to promote and enhance multistakeholder processes for the governance of the internet, including ICANN and at the Internet Governance Forum (IGF). These efforts will be complemented by our work to shape global digital technical standards (described in the Technology chapter) and our work to expand UK cyber security exports (set out below) which will also help to embed UK standards into the cyber ecosystems of other nations.

**163. Most 'middle ground' countries support and promote the UK's vision for cyberspace and the future of the internet, more successfully countering the influence of authoritarian states over the multi-stakeholder system.** We will demonstrate that it is possible to address challenges in cyberspace without adopting authoritarian approaches while also enabling innovation, development and growth. We will support countries grappling with digitalisation to build the full range of legal and strategic communications expertise they need to engage with the international debate and to implement agreed frameworks. We will continue to expose irresponsible use of cyber capabilities, building trust internationally. And we will continue to demonstrate an open and transparent approach to our use of offensive cyber capabilities wherever we can, reinforcing the UK's reputation as a force for good.

## Objective 3: Leverage and export UK cyber capabilities and expertise to boost our strategic advantage and promote our broader foreign policy and prosperity interests.

**164.** In response to systemic competition and rapid technological change, UK cyber activity and capabilities will be considered alongside other sources of national power to bolster our strategic advantage and promote our foreign policy and prosperity goals. Our aim is to achieve an international order in which open societies and economies can flourish and human rights are defended, whilst driving prosperity at home. We will achieve the following outcomes by 2025:

**165.** Our activity in and in relation to cyberspace has **enhanced global stability and protected the rules-based international system, open societies and democratic systems where they are being undermined**. We will deliver an international values-based campaign to champion human rights, diversity, and gender equality in the design, development and use of cyberspace. This will include but not be limited to tackling internet shutdowns, bias in Artificial Intelligence algorithms and increasing online safety. We will compete more effectively to protect democratic values, systems and processes and strengthen the rules-based international system (including the United Nations, World Health Organisation and the global trading system) by investing further in our network of cyber officers that stretch across six continents. We will enhance our use of strategic communications to promote UK research collaboration and academic exchange programmes and help to ensure UK ideas translate into practical applications.

**166. The UK is one of the top 3 global exporters of cyber solutions and cyber expertise**, with our cyber industry regarded as the 'go-to' provider of cyber security solutions for foreign government and major commercial clients. We will showcase the best of UK cyber security through more active international government-to-government engagement, under the auspices of the UK Cyber Security Ambassador Programme and our international network. We will support companies across the UK at every stage of the innovation to export pathway to become competent exporters and attract inward investment and provide more support to SMEs, including through a new Export Faculty.[32] [33] Alongside our work through the Cyber Growth Partnership and other efforts outlined in the UK Cyber Ecosystem chapter we will also develop a new Cyber Capability Campaign Office to provide more structured and coordinated support to major export campaigns.

[32] Described in the UK Innovation Strategy (2021)

[33] The UK Defence & Security Exports (UKDSE) Export Faculty is an online learning and development hub aimed at SMEs in the defence and security sector with specific modules for cyber security companies. Registering for the Faculty provides access to a programme of curriculum based learning modules and in addition, valuable information around UK Defence and Security Exports planned events and activities.

## Charles Juma, UK Digital Access Programme in Nairobi

My name is Charles Wesonga Juma. I lead, shape and deliver cyber security, digital development, inclusion, and entrepreneurship as part of the global and cross-government UK Digital Access Programme in Kenya. I also support complementary projects under the Conflict, Stability and Security Fund (CSSF) Cyber Portfolio. The importance of online safety, security, data protection and responsible use of cyberspace cannot be overemphasised. As we have learnt from the COVID-19 pandemic, online safety and hygiene can be as important as public health and hygiene. I am passionate about ensuring that everyone is protected from online threats and harms as part of the UK government's overall cyber power.

## Sara Merchant, Cyber Officer at the British Embassy, Tbilisi

I'm Sara and I'm posted to the British Embassy Tbilisi as our Cyber Officer, working closely with the Georgian Government and NCSC UK. My day-to-day work varies from political engagement, to supporting implementation of the new cyber strategy, to leveraging UK specialists to increase Georgia's technical capability. I feel privileged to be at the forefront of projecting UK expertise and supporting Georgia to build up resilience against cyber threats. As a country who has, unfortunately, a great deal of experience in being on the sharp end of hostile state activity there is a lot we can learn here in Georgia. Our work makes us both stronger, more resilient, and better informed.

# Pillar 5: Countering Threats

# Detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace

**167.** The nature of the threat we face is complex. We are concerned about threats in cyberspace (for example to our online activities), threats to the UK and partners through cyberspace (for example to networked UK critical national infrastructure), and threats to the functioning of underpinning international cyber infrastructure. All of these threats can impact the availability of services that people rely on, or the confidentiality or integrity of data and information that passes through those systems. The foundations of our approach to countering the threat are in promoting cyber resilience as outlined earlier in this document. This chapter focuses on how we will raise the costs and risks of attacking the UK in cyberspace and ensure we achieve our full potential as a cyber power.

**168.** Since the National Cyber Security Strategy 2016-2021, we have transformed our approach to mitigating the threat. We have established world class cyber threat detection and analysis capabilities as part of the National Cyber Security Centre (NCSC). The NCSC works with partners across the public and private sector, at home and overseas, to detect and respond to threats and incidents. As part of the wider intelligence community the NCSC has also been able to inform policy makers on the attribution of attacks against UK interests, which is a critical part of our approach to deterring cyber threats. We have significantly invested in our offensive cyber capabilities, through the National Offensive Cyber Programme and now the new National Cyber Force (NCF). We have also developed an integrated National Crime Agency (NCA)-led national law enforcement response and have sought to disrupt and raise the cost of hostile and criminal activity in cyberspace. We have created world class threat detection and assessment capabilities with the means to translate the resultant insight into impactful mitigations across the public and private sector. And we have developed an autonomous cyber sanctions regime as another lever to impose costs on hostile actors. In combination, our diplomatic engagement, the NCSC, our security and intelligence agencies, the NCA, wider law enforcement and the NCF have reduced the real-world impact caused by threats, by taking action to directly counter adversaries, help prevent attacks, and reduce harm.

**169.** But the threats have also grown in sophistication, complexity and severity; and our efforts have not yet fundamentally altered the risk calculus of attackers who continue to successfully target the UK and its interests. Cyber attacks against the UK are motivated by espionage, criminal, commercial, financial and political gain, sabotage and disinformation. Attackers develop capabilities that evade mitigations; increasingly sophisticated cyber tools and related enablers have been commoditised in a growing industry, lowering the barriers to entry for all types of malicious actors. And rewards are increasing as the ability of actors to steal and encrypt valuable data and extort ransomware payments continues to grow, disrupting businesses and key public services. The result has seen attackers increasingly benefit financially, exploit privacy and freedom of speech, and attempt to manipulate events through disinformation.

**170.** The UK's approach will therefore now shift to a more integrated and sustained campaign footing that will involve making routine, integrated and creative use of the full range of levers and capabilities available to impose costs on our adversaries, pursue and disrupt perpetrators and deter future attacks. The key supporting elements of this approach will be:

- the continued development of the NCF as the next step in the UK's ability to conduct offensive cyber operations against its adversaries
- tailored cross-government campaigns to tackle threats to the UK – making use of our diplomatic, military, intelligence, law enforcement, economic, legal and strategic communications tools
- new investment to enable law enforcement to pursue investigations at scale and pace and to maintain a technical edge over our adversaries in order to prevent and detect serious criminals and the enabling services they rely upon
- a major step up in data sharing across government and industry as outlined in the Resilience chapter

**171.** Cyberspace presents opportunities for the UK, creating new ways to actively pursue our national interests. For example, offensive cyber operations offer us a range of flexible, scalable, and de-escalatory measures that will help the UK to maintain our strategic advantage and to deliver national priorities, often in ways that avoid the need to put individuals at risk of physical harm.

**172.** We will continue to develop and invest in our offensive cyber capabilities, through the NCF. The NCF will transform the UK's ability to contest adversaries in cyber space and the real world, to protect the country, its people and our way of life. These capabilities will be used responsibly as a force for good alongside diplomatic, economic, criminal justice and military levers of power. They will be used to support and advance a wide range of government priorities relating to national security, economic wellbeing, and in support of the prevention and detection of serious crime.

## Objective 1: Detect, investigate and share information on state, criminal and other malicious cyber actors and activities in order to protect the UK, its interests and its citizens

**173.** We will achieve the following outcomes by 2025:

**174. The government has a comprehensive understanding of the cyber capabilities of state, criminal and other malicious cyber actors and their strategic intent towards the UK.** We will sustain and grow the considerable investments made under the 2016 strategy in the intelligence agencies and law enforcement for understanding the cyber threat. In particular, we will increase law enforcement's capability to understand and tackle the cyber crime threat, including its links to state and other international and domestic threats and its technological enablers, helping us to develop more effective policy responses. We will improve how we coordinate threat detection across government, with a joint data access and exploitation strategy across the intelligence agencies and law enforcement. And we will focus even more on understanding the intent and decision-making criteria of our adversaries and the impact our activities are having on them, including how individuals become cyber criminals and what action we can take to prevent this from happening.

**175.** Our work to enable faster and easier reporting of cyber incidents and crimes, outlined in the Resilience chapter will also help to achieve this outcome.

**176. Most serious state, criminal and other threats are routinely and comprehensively investigated**, drawing on all sources of information and bringing together expertise across government, law enforcement and the private sector. We will build the intelligence, operational and technical capabilities of the UK's law enforcement cyber network. We will invest in the NCA's cyber intelligence capability, used to target organised crime groups, the regional intelligence build initiative, which will enhance intelligence access and movement across the UK, and the skills and capability that law enforcement need to investigate and disrupt cyber and digital crimes.

**177.** Investigations will be supported by intelligence from all sources and leverage skills and knowledge across the private sector, including by helping businesses to share data more easily with law enforcement. And we will continue to implement the recommendations of the HMICFRS on the policing response to cyber crime to ensure the cyber crime network at the national, regional and local levels remains on a secure footing.[34]

[34] Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services

**178. Information and data on the threat is routinely shared at scale and pace and those who receive it are more able to take action.** The NCSC has trialled a range of initiatives to build up more effective communities of network defenders, across a wide variety of sectors, who not only receive and are able to share threat information, but are increasingly capable at using it for collective benefit. We will expand this work, with an initial focus on helping government defend itself better, supported by the Government Cyber Coordination Centre (described in the Resilience chapter). The Financial Sector Cyber Collaboration Centre is already leading the way in the private sector.[35]

**179.** The NCSC are also investigating ways to track emerging threats and continue to work with the Alan Turing Institute to explore whether machine learning can be used to detect certain types of cyber attack. This research will continue to improve our understanding of how we can use artificial intelligence to detect malicious activity.

[35] NCSC, Financial sector cyber collaboration centre (FSCCC) (2021)

# Stopping cyber crime also means tackling other types of criminal activity

Cyber crimes (defined as Computer Misuse Act offences) occur when there is unauthorised access to computers, networks, data and other digital devices, associated acts that cause damage or the making or supplying of tools to commit these offences. This can allow cyber criminals to commit further malicious cyber activities such as ransomware attacks, unauthorised account access, intellectual property theft, denial of service attacks, or the stealing of large personal data sets – these are significant and growing crimes.

For citizens, cyber crimes often manifest in the further crimes they enable and facilitate. Unauthorised computer access can lead to a wide range of frauds, theft, sextortion, and in some cases facilitate stalking, domestic abuse and harassment. All of these crimes cause significant harm to UK citizens on a daily basis, destroying businesses and ruining lives. Cyber crimes are therefore distinct and different from wider online safety issues such as bullying and harassment, hate speech, the spreading of disinformation, promotion of gang culture and violence, or underage access to pornography. The government is addressing these issues through the online harms white paper and draft online safety bill.

## Objective 2: Deter and disrupt state, criminal and other malicious cyber actors and activities against the UK, its interests, and its citizens.

**180.** We will achieve the following outcomes by 2025:

**181. It is more costly and higher risk for state, criminal and other malicious cyber actors to target the UK**. We will implement sustained and tailored deterrence campaigns that leverage the full range of UK capabilities (including diplomatic, economic, covert and overt levers) to influence the behaviour of malicious and criminal cyber actors. In particular we will improve our signalling to adversaries of our capability and willingness to impose meaningful costs, including through sanctions, law enforcement and NCF operations. And through NCA's Cyber Choices programme we will divert individuals from becoming involved in cyber crime, working with industry and academia to offer potential offenders better alternatives such as apprenticeships and work placements.

**182.** We will also provide the tools and powers law enforcement and the intelligence agencies need through the Counter State Threats Bill, by updating existing legislation and introducing new offences to account for how state threats have evolved. And we will amend the Proceeds of Crime Act 2002 to optimise law enforcement's ability to identify, seize and recover the proceeds of cyber crime. In particular, we will do this by creating a civil forfeiture power to mitigate the risks posed by those who cannot be prosecuted.

**183. State, criminal and other malicious cyber actors are less able to target the UK as a result of our disruption and denigration of their activities and capabilities**. We will review the government's policy and operational approach to tackling ransomware, adopting this as one of our priority campaigns, collaborating with industry and our international partners. We will maximise the partnerships between the NCF, NCSC, NCA and wider law enforcement and the diplomatic and intelligence communities to counter threats that disrupt the confidentiality, integrity and availability of cyberspace or data and services in cyberspace. In particular we will invest in capabilities to target cybercriminal infrastructure and deploy our law enforcement and offensive cyber capabilities to disrupt malicious cyber activity. Our adversaries are building cyber capabilities and increasingly using them for malign purposes. We will make full use of the NCF, where we deem it appropriate, to disrupt these efforts and defend and protect the UK.

**184.** We will also counter the proliferation of high-end cyber capabilities to states and organised crime groups via commercial and criminal marketplaces, tackling forums that enable, facilitate, or glamorise cyber criminality.

**185. An increase in criminal justice and other disruptive outcomes for cyber criminals** with improved criminal justice capability used to prosecute cyber criminals in the UK. We will review the Computer Misuse Act (CMA) and relevant powers to ensure that law enforcement agencies have the ability to investigate new and emerging threats from criminals and introduce more specialist prosecutors to deal with the increasing number of cyber cases. We will also improve specialist law enforcement skills, exercising and mainstreaming to ensure a continuing supply of officers with required cyber specialist knowledge, through the National Police Chiefs' Council (NPCC) cyber skills prospectus and the College of Policing Cyber Digital Career Pathways.

**Susan Moody, Police Service of Northern Ireland (PSNI) Prevent Officer**

L-R Susan Moody (PSNI), Sarah Travers (TV presenter) and Joe Dolan (Head of the Northern Ireland Cyber Security Centre)

Computers and mobile devices are part of a young person's everyday life. They provide great opportunities but also dangers if misused. The prevent function within PSNI provides a much needed early intervention with young people and helps them understand the law around using and misusing computers. This highlights the danger signs for potential criminal activity and also highlights the great opportunities through initiatives such as CyberFirst and cyber as a career, which can give those who have a curiosity or talent an alternative to offending, and prevent abuse by others for criminal ends. Susan has worked tirelessly in developing a schools cyber information programme available for all secondary schools and has engaged directly with more than 40 primary schools, numerous secondary schools, young people's organisations and uniformed groups. These young people could well be our cyber ambassadors and defenders of the future.

## Objective 3: Take action in and through cyberspace to support our national security and the prevention and detection of serious crime

**186.** We will achieve the following outcomes by 2025:

**187. The UK's cyber capabilities have a greater impact in deterring and disrupting non-cyber threats**. We will scale-up and develop the NCF, delivering on our long-term vision for this key capability, ensuring that it is fully integrated with GCHQ, MOD, SIS and Dstl and working closely with law enforcement and wider government. We will deliver legal and proportionate offensive cyber operations through the NCF, acting responsibly in cyberspace and leading by example. Offensive cyber operations will continue to support the UK's national security, including our defence and foreign policy, and in the prevention of serious crime.

**188.** We will also scale up and develop law enforcement technical capabilities against infrastructure and cryptocurrency, which can be deployed against other threats.

**189. UK cyber capabilities are integrated across the full breadth of defence operations** in line with the Integrated Operating Concept 2025.[36] This will maintain our competitive warfighting edge over adversaries and enable greater collaboration with our allies and partners. We will continue to progress the Defence Multi-Domain Integration Change Programme, which will bring together capabilities across the domains, and deliver greater integration with other instruments of our national power, bolstering our military advantage over our adversaries. Cyber will be a mainstream part of defence business enabled by highly skilled cyber specialists, an overall cyber awareness across the defence workforce and cutting-edge and resilient cyber capabilities.

[36] Ministry of Defence, Integrated Operating Concept (2020)

# Major law enforcement cyber crime investigations

**Operation Imperil**: Op Imperil was a joint South East Regional Organised Crime Unit (SEROCU) investigation with the FBI into a website selling compromised personal and banking information of victims of cyber-attacks. This enabled others to purchase personal data to commit frauds and further computer misuse offences. Significant investigation led to the identification of bank accounts and payments used for the technical infrastructure, identifying that the website owner was based in Pakistan. This enabled the FBI to covertly seize the website and then subsequently take it down. The South East Regional Organised Crime Unit arrested the primary UK suspect who was discovered to have opened a US based bank account on behalf of the website owner for the laundering of criminal funds. The UK suspect committed significant fraud using some of the compromised victim data, opening bank accounts in other names, utilising compromised bank accounts to pay for luxury holidays and false Department of Work and Pensions claims resulting in a loss to the state of in excess of £90,000. The suspect was charged with nine counts and sentenced to four years imprisonment reduced due to an early guilty plea. The judge awarded the investigative team a Judge's Commendation. Confiscation and a lifetime Proceeds Of Crime Act application is in progress at time of publication.

**Operation Nipigon**: This was a Met Police investigation into a Bulgarian National who was suspected of creating bespoke phishing pages estimated to have caused losses to the UK in excess of £40 million. He was identified following an investigation into another well known cyber criminal previously sentenced to 10 years custodial in 2018, who was using the phishing pages created by the Bulgarian National to enable his own criminality. The investigation was opened following the identification of a significant email address linked to the suspect which after a number of protracted and complex enquiries led to engagement with the Bulgarian authorities and the suspect was arrested, extradited and following comprehensive disclosure, pleaded guilty to all criminal charges receiving a nine and a half year custodial sentence.

**Operation Leasing:** In 2020, the NCA led an investigation into terrorist bomb threats made against the NHS at the height of the COVID-19 pandemic, demanding payments in Bitcoin (BTC). Working with German authorities, the NCA identified and apprehended the suspect, who was successfully convicted in a German court.

On 12th April 2020, an Italian national, living in Germany, sent an email via the TOR network stating his intention to bomb an NHS hospital unless he received £10 million in Bitcoin.

This was rapidly identified as a high-priority by the NCA and specialist cyber crime officers were tasked to identify the perpetrator and prevent any potential attack.

The perpetrator had also sent emails threatening to attack MPs and bomb Black Lives Matter protestors in London. Despite writing his emails in English, NCA investigators used specialised cyber techniques and behavioural and linguistic analysis to deduce that the offender was likely a native German speaker.

In collaboration with German authorities, NCA officers identified that the emails were sent from a computer at an address in Berlin. Through international collaborative working, and despite significant efforts to mask his identity and location, the suspect was identified and placed under surveillance by German law enforcement. On 15 June 2020 the suspect was arrested, charged with attempted extortion and remanded in custody. He was convicted on 26 February 2021 and sentenced to three years in prison.

# Taking action through cyberspace to counter terrorism

**Counter Daesh campaign:** MOD and GCHQ's work against Daesh is an example of how we have taken active steps to counter threats from those who misuse the power of the internet and modern communications.

Daesh devoted much time and energy to technology, to create media content used to radicalise and attract new recruits and to inspire terrorist attacks around the world. In recent years we've seen the impact of this approach all over Europe, including attacks in London and Manchester. Daesh also used modern communications systems to command and control their battlefield operations. This allowed them to operate flexibly, at scale and pace, and to pose an even greater danger to the populations they sought to control, and to maximise their reach across their so-called caliphate.

During the Battle of Mosul, the self-declared capital of Daesh, we used cyber tools and techniques in operations alongside the military in support of the coalition and as part of a wider, full-spectrum campaign. The outcomes of these operations were wide-ranging. Disruption of communications, degradation of propaganda, causing distrust within groups, and denial of equipment and networks used as part of their operations were all ways in which Daesh's effectiveness could be reduced. We could also use cyber techniques to promote UK government messaging to targets, or to highlight their activities to those who may unsuspectingly be providing them with assistance. These operations made a significant contribution to coalition efforts to suppress Daesh propaganda, hindered their ability to coordinate attacks, and protected coalition forces on the battlefield.

## Andrew, a member of the National Cyber Force

I've always been fascinated by the latest cutting-edge technology. Before working for the intelligence services, I joined the police and worked my way up from a Constable on the beat to specialising in digital forensics – looking at suspects' electronic devices for evidence. I loved it but wanted to see what other opportunities were out there.

I didn't go to university after leaving school and my career so far has been led by a natural curiosity, and that's true of all my colleagues who are joining the National Cyber Force. They come from all kinds of backgrounds. You have deep technical experts at the heart of it all, as well as a former supermarket branch manager, a primary school teacher and a fire fighter. The one thing we all have in common is an open mind, a hunger to learn and a shared goal of keeping the country safe – seeing both the threats and opportunities for national security from emerging technology.

As a police officer I was immensely proud to help people on a personal level. Today, as part of this unique team at the National Cyber Force, I'm part of a force for good on a global scale.

# Delivering Our Ambition

**190.** This strategy will mean nothing without a rigorous approach to implementing its objectives, monitoring and evaluating progress against them, and having the mechanisms to adjust course where necessary. This chapter sets out our approach to delivery.

## Roles and responsibilities across Government

**191.** The National Cyber Strategy will be one of the sub-strategies that will collectively deliver the ambitions of the Integrated Review. The National Security Council will exercise ministerial oversight of these strategies, monitoring implementation and considering the overall balance and direction of UK strategy. Progress against the objectives of the strategy will also be assessed via the Government Planning and Performance Framework and Outcome Delivery Plans.

**192.** All ministers play a role in ensuring that the UK cements its position as a responsible and democratic cyber power, able to protect and promote its interests in and through cyberspace. This list includes specific sets of responsibilities for ministers in leading roles, either for implementing or coordinating one or more of the five pillars of our National Cyber Strategy or overseeing our most important cyber capabilities and decisions.

- **The Chancellor of the Duchy of Lancaster,** supported by the **Paymaster General**, provides overall leadership across departments to ensure an effective government response to cyber threats, and fulfilment of our ambitions as a cyber power. This includes the development and implementation of the National Cyber Strategy, the supporting programme of investment and coordination of the government's efforts on cyber resilience. They also have overall cross-sector policy and coordination responsibility for the

cyber security and resilience of the UK's critical national infrastructure. The Chancellor of the Duchy of Lancaster is the default chair for ministerial COBR meetings on cyber incidents, when these are necessary.

- **The Secretary of State for the Home Department** has a key role in the delivery of the National Cyber Strategy as a whole, and in the response to cyber incidents in line with their responsibilities for homeland security. They lead the government's work to detect, disrupt and deter our adversaries alongside the Secretary of State for Foreign, Commonwealth and Development Affairs and the Secretary of State for Defence and provide overall coordination of that work. They also have specific responsibility to counter cyber crime.
- **The Secretary of State for Foreign, Commonwealth and Development Affairs** has statutory responsibility for GCHQ and thus for the National Cyber Security Centre. They lead the government's work to advance UK global leadership on cyber and have specific responsibility for the cyber attribution process, cyber sanctions regime and international engagement for high category cyber incidents. They also lead the government's work to detect, disrupt and deter our adversaries alongside the Secretary of State for the Home Department and the Secretary of State for Defence.
- **The Secretary of State for Defence** leads the government's work to detect, disrupt and deter our adversaries alongside the Secretary of State for Foreign, Commonwealth and Development Affairs and the Secretary of State for the Home Department.
- **The Secretary of State for Foreign, Commonwealth and Development Affairs and the Secretary of State for Defence** have responsibility for the National Cyber Force, as a joint endeavour between defence and intelligence.
- **The Secretary of State for Digital, Culture, Media and Sport** leads on the cyber security of organisations in the wider economy as it relates to digital policy, and the relevant growth, innovation and skills aspects of the National Cyber Strategy. They lead the government's work to strengthen the UK's cyber ecosystem and to take the lead in technologies vital to cyber power.
- **Ministers of all Lead Government Departments for critical national infrastructure** have responsibility for the cyber security and resilience policy for their sectors.
- **All ministers** should provide oversight of the cyber security of their departments and implementation of appropriate mitigations. Where a department oversees an element of the public or private sector (for example DLUHC and local government or DEFRA and the water companies) they are responsible for the cyber policy and assurance activities relating to that sector.

**193.** The Deputy National Security Adviser for Intelligence, Security and Resilience is the Senior Responsible Owner for the strategy and will lead delivery across government at official level, supported by the relevant senior officials across departments.

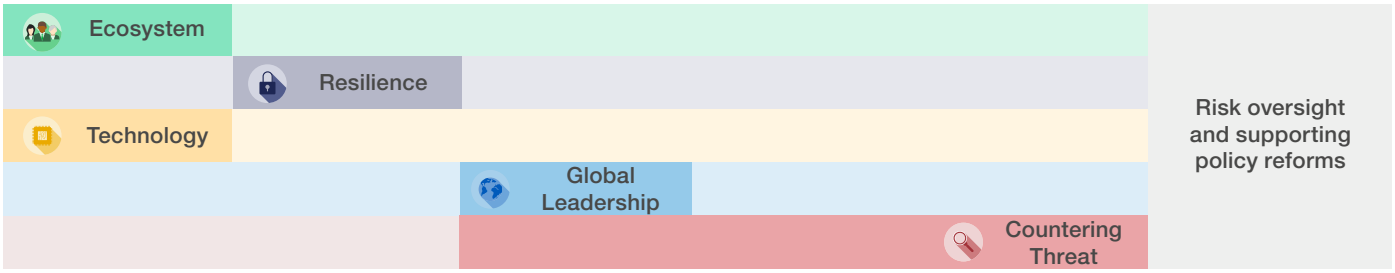
National Cyber Strategy

# Ministerial Responsibilities

## Prime Minister

| Digital Secretary | Chancellor of the Duchy of Lancaster* | Foreign Secretary | Defence Secretary | Home Secretary | All Secretaries of State |
|---|---|---|---|---|---|

**Coordination and leadership of the strategic pillars**




**Operations and delivery support across the strategy**


*provides overall leadership across departments to ensure an effective government response to cyber threats, and fulfilment of our ambitions as a cyber power.

## Investing in our cyber power

**194.** The government will be investing £2.6 billion in cyber and legacy IT over the next three years. This is in addition to significant investment in the National Cyber Force. It includes a £114 million increase in the National Cyber Security Programme with annual spending on capability built under the 2016 strategy moved under departmental management and put on a permanent footing. International programmes will be delivered via the Conflict, Stability and Security Fund (CSSF) to assist partner countries, build their cyber resilience and counter cyber threats. This is alongside increases in investment also announced in R&D, intelligence, defence, innovation, infrastructure and skills, all of which will contribute in part to the UK's cyber power.[37]

## Measuring success

**195.** The strategy will be governed by a continuously evolving performance framework that reports to senior responsible officials and the National Security Council. The framework will be used to inform discussions with parliamentary and other bodies that oversee the national security community's work. Consistent with the approach of the National Cyber Security Strategy 2016-2021, it will not be a public document due to the sensitive information contained but the government will publish annual progress reports.

**196.** This performance framework will:

- Provide a clear pathway of how activities will lead to the various objectives outlined in the strategy
- Ensure accountability for the delivery of the strategy
- Provide transparency on the progress the country is making towards the goals set out in the strategy
- Illustrate how activity needs to adapt to bring it in line with the strategy
- Understand what activities are effective in achieving strategic ambitions, so that these lessons can be applied in the future
- Provide a holistic view of activity across the five pillars, reducing duplication and identifying strengths and weaknesses within the country's cyber power
- Ensure the strategy is providing cyber support to all sections of society

[37] HM Treasury, Autumn Budget and Spending Review 2021 (2021)

## Next steps

**197.** This strategy is intended as a guide for action, not only for those in government who have responsibility for cyber and the wide range of other related policies (see Annex A) but also for every person and organisation across the whole of our society with an interest in and responsibility for our national cyber effort. It is also the beginning of a conversation that we want to continue, to ensure our objectives and priorities remain relevant over the next five to ten years. We will use the publication of this strategy as a platform for further engagement with the public, private and third sectors across the UK and invite direct feedback to ukcyberstrategy@cabinetoffice.gov.uk. We will report back annually on the progress we are making to implement this strategy.

# Annex A: Cyber as part of the government's wider agenda

The National Cyber Strategy is intended to support and amplify a range of other priorities for the Government across security, defence, foreign policy and our economic agenda. In turn, this strategy will rely on the broader capabilities developed through our education and skills system and our national approach to digital and technology industrial policy, research and business growth. Key relevant strategies and plans include:

- **The Integrated Review**, including national efforts to improve resilience, tackle state threats, serious organised crime and terrorism, sustain our strategic advantage through science and technology and shape the international order
- **The National Data Strategy**, which sets out our vision to harness the power of responsible data use to boost productivity, create new businesses and jobs, improve public services, support a fairer society, and drive scientific discovery, positioning the UK as the forerunner of the next wave of innovation.This includes transforming the government's use of data to drive efficiency and improve public services by addressing barriers to data sharing between departments and improving the quality of the data they hold. This will be essential in supporting our cyber agenda such as ensuring we are able to collate and use good quality data on cyber incidents
- **The plan for growth,** which is helping us to **Build Back Better** through additional support and investment for infrastructure, skills and innovation and the **Innovation Strategy**, which sets our ambitions for an innovation-led economy
- **The Plan for Digital Regulation**, which sets out our pro-innovation approach to regulating digital technologies in a way that drives prosperity and builds trust in their use
- **The National AI Strategy**, which aims to prepare the UK for the coming transformative decade in AI by investing in the long-term needs of the AI ecosystem, supporting the transition to an AI-enabled economy, and ensuring the UK gets the national and international governance of AI technologies right. This also includes measures to support cyber-secure innovation in AI-enabled systems while protecting the public and building trust in its use
- The forthcoming **National Resilience Strategy**, which will in part focus on how the UK will stay on top of technological threats and remain resilient in cyberspace
- The forthcoming **Digital Strategy**, which will set out a clear vision of the government's ambitions to harness new appetite for digital transformation, accelerate growth, and continue to build a more inclusive, competitive and innovative digital economy for the future;which will build on DCMS's Ten Tech Priorities to further set out the government's ambitions in the digital sector
- **The Net Zero Strategy,** ensuring our prosperous, innovation-led economy is a low carbon one
- **The Beating Crime Plan**, which sets out how we will restore confidence in the criminal justice system and deliver our shared vision of a safer Britain with less crime and fewer victims[38]

[38] Home Office, Beating Crime Plan (2021)

Directly supporting the National Cyber Strategy are two further publications that set out how individual parts of the strategy will be met.

- The forthcoming **Government Cyber Security Strategy**, which will set out more detailed plans for improving the security of government and the public sector, in support of this national strategy
- The forthcoming **Incentives & Regulations Review 2021**, which will set out our findings on how effective our work to incentivise improvements in cyber security within the wider economy have been, and how we propose to implement the business and organisational elements of the resilience pillar

# Annex B: NIS Regulations – National Strategy

## Introduction

### NIS National Strategy

**1.** The National Cyber Strategy is designated as the UK's national strategy for the purposes of Regulation 2 of the UK Network and Information Systems (NIS) Regulations 2018.

**2.** This annex provides further information including:

- the roles and responsibilities of key authorities responsible for NIS implementation in the UK; and
- a list of the key authorities involved.

### UK NIS Regulations

**3.** In 2016, the European Commission agreed a Directive with the aim of increasing the security of Network and Information Systems within the European Union (EU). This was supported by the UK Government.

**4.** On 20 April 2018, the Government laid the new Network and Information Systems (NIS) Regulations 2018 in Parliament. These Regulations came into force on 10 May 2018.

**5.** The NIS Regulations established a new regulatory regime within the UK that requires designated operators of essential services (OESs) and relevant digital service providers (RDSPs) to put in place technical and organisational measures to secure their network and information systems.

**6.** It applies to sectors which are vital for our economy and society and which rely heavily on network and information systems; energy, transport, drinking water, healthcare and digital infrastructure.

**7.** Key digital service providers (search engines, cloud computing services and online marketplaces) are also covered.

**8.** The NIS Regulations establish:

- **a national framework** to support the implementation, including a national strategy;
- sector-specific **competent authorities** acting as regulators;
- the National Cyber Security Centre (NCSC) as the **Single Point of Contact** (SPOC) and **Computer Security Incident Response Team** (CSIRT).

**9.** Progress is assessed through Post-Implementation Reviews every 2-5 years.

## Key roles and responsibilities

### National Framework

**10.** The Cabinet Office is responsible for the National Cyber Strategy, which comprises the NIS National Strategy. The Cabinet Office also has overall responsibility for improving the security and resilience of critical national infrastructure.

**11.** The Department for Digital, Culture, Media and Sport (DCMS) is responsible for the overall implementation of the NIS Regulations, including co-ordinating the relevant authorities and NCSC. DCMS issues guidance for competent authorities to support wider NIS implementation across the UK.

### Single Point of Contact (SPOC)

**12.** The national contact point for engagement with international [EU] partners on NIS, coordinating requests for action or information and submitting annual incident statistics. The National Cyber Security Centre is the UK's SPOC.

### Computer Security Incident Response Team (CSIRT)

**13.** The National Cyber Security Centre is the UK's CSIRT. It is responsible for monitoring cyber security incidents at a national level; providing real-time threat analysis, defence against national cyber-attacks, technical advice, and response to major cyber incidents to help minimise harm.

**14.** NCSC maintains the outcome-based Cyber Assessment Framework (CAF) and provides extensive guidance on cyber security matters as National Technical Authority.

### Competent Authorities

**15.** These are responsible for oversight and enforcement of the NIS Regulations in their sectors, designating and assessing the compliance of OESs and RDSPs to the requirements of the NIS Regulations. They are set out in Schedule 1 of the NIS Regulations and a list is provided in section 3.

## Operators of Essential Services (OESs) and Relevant Digital Service Providers (RDSPs)

**16.** OESs or RDSPs which meet the designation thresholds for that sector, or have been designated by the relevant authority under Regulation 8(3) of the NIS Regulations, must comply with the requirements of the NIS Regulations.

**17.** These involve:

- taking appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems;
- taking appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems;
- notifying the relevant competent authority about any incident which has a substantial impact on their services;
- meeting the inspection requirements under the NIS Regulations; and
- complying with information, enforcement, and penalty notices.
- RDSPs are also required to register with the ICO.

## Other relevant authorities:

**18.** The UK Government works closely with the Devolved Administrations and other relevant authorities, including Lead Government Departments, on the implementation of the NIS Regulations.

**19.** The Centre for the Protection of the National Infrastructure (CPNI) provides advice on related physical and personnel security.

## List of key authorities for NIS implementation

| National Authorities | |
|---|---|
| UK NIS Regulations | Department for Digital, Culture, Media and Sport |
| UK National Cyber Strategy | Cabinet Office |
| UK Single Point of Contact (SPOC) | National Cyber Security Centre |
| UK Computer Security Incident Response Team (CSIRT) | National Cyber Security Centre |

| Competent Authorities | | | | | |
|---|---|---|---|---|---|
| **Sector** | **Subsector** | **England** | **Wales** | **Scotland** | **Northern Ireland** |
| **Energy** | Electricity | Joint: Department for Business, Energy, and Industrial Strategy and the Gas and Electricity Markets Authority (Ofgem) | | | Department of Finance |
| | Oil | Department for Business, Energy, and Industrial Strategy | | | Department of Finance |
| | Gas | Joint: Department for Business, Energy, and Industrial Strategy and the Gas and Electricity Markets Authority (Ofgem)[39] | | | Department of Finance |
| **Transport** | Air | Joint: Department for Transport and The Civil Aviation Authority (CAA) | | | |
| | Rail | Department for Transport | | | Department of Finance |
| | Water | Department for Transport | | | |
| | Road | Department for Transport | | Scottish Ministers | Department of Finance |
| **Healthcare** | Healthcare settings | Department of Health and Social Care | Welsh Ministers | Scottish Ministers | Department of Finance |
| **Drinking Water** | Drinking Water | Department for Environment, Food and Rural Affairs | Welsh Ministers | Drinking Water Quality Regulator for Scotland | Department of Finance |
| **Digital Infrastructure** | Digital Infrastructure | Office of Communication (Ofcom) | | | |

[39] For certain exceptions the Department for Business, Energy, and Industrial Strategy is the sole Competent Authority. For further detail see Schedule 1 and 2 of the Network and Information Systems Regulations 2018.

# Annex C: Glossary

**Action Fraud –** the reporting centre for fraud and cyber crime where citizens and organisations should report fraud if they have been scammed, defrauded or experienced cyber crime in England, Wales and Northern Ireland. In Scotland, reports go to Police Scotland.

**Active Cyber Defence (ACD) –** helps organisations to find and fix vulnerabilities, manage incidents or automate disruption of cyber-attacks. Some 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.

**Artificial Intelligence –** a technology in which a computing system is coded to "think for itself', adapting and operating autonomously. AI is increasingly used in more complex tasks, such as medical diagnosis, drug discovery, and predictive maintenance.

**Authentication –** the process of verifying the identity, or other attributes of a user, process or device.

**Autonomous System –** a collection of IP networks for which the routing is under the control of a specific entity or domain.

**Blockchain Technology –** a particular way of storing data. A blockchain is an example of a distributed ledger – a type of append-only, tamper-proof storage technology.

**COBR –** Cabinet Office Briefing Rooms. The UK central government response to emergencies is underpinned through use of COBR; the physical location, usually in Westminster, from which the central response is activated, monitored and co-ordinated and which provides a focal point for the government's response and an authoritative source of advice for local responders.

**Competent Authorities –** regulatory bodies as described in the Network and Information Systems (NIS) Regulations 2018. There are multiple competent authorities responsible for different sectors covered by NIS.

**Connected Places –** a community that integrates information and communication technologies and IoT devices to collect and analyse data to deliver new services to the built environment, and enhance the quality of living for citizens.

**Critical National Infrastructure –** Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:

a. major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or

b. significant impact on national security, national defence, or the functioning of the state.

**Crypt-Key (CK) –** the term used to describe the UK's use of cryptography to protect the critical information and services on which the UK government, military and national security community rely, including from attack by our most capable adversaries.

**Cryptocurrency –** a digital currency and payment system, e.g. Bitcoin.

**Cryptography –** the science or study of analysing and deciphering codes and ciphers; cryptanalysis.

**Cyber Assessment Framework (CAF) –** provides a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation responsible.

**Cyber Attack –** deliberate exploitation of computer systems, digitally-dependent enterprises and networks to cause harm.

**Cyber crime –** cyber-dependent crime (crimes that can only be added] committed through the use of ICT devices, where the devices are both the tool for committing the crime and the target of the crime); or cyber–enabled crime (crimes that may be committed without ICT devices, like financial fraud, but are changed significantly by use of ICT in terms of scale and reach).

**Cyber ecosystem –** the totality of interconnected infrastructure, persons, processes, data, information and communications technologies, along with the environment and conditions that influence those interactions.

**Cyber Incident –** an occurrence that actually or potentially poses a threat to a computer, internet-connected device, or network – or data processed, stored, or transmitted on those systems – which may require a response action to mitigate the consequences.

**Cyber Resilience –** The overall ability of systems, organisations and citizens to withstand cyber events and, where harm is caused, recover from them.

**Cyber Risk –** The potential that a given cyber threat will exploit the vulnerabilities of an information system and cause harm.

**Cyber Security –** The protection of internet-connected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so.

**Cyber Security Body of Knowledge (CyBOK) –** A unique resource, providing for the first time an underpinning body of knowledge encompassing the breadth and depth of cyber security, showing that cyber security encompasses a wide range of disciplines.

**Cyber Threat –** anything capable of compromising the security of, or causing harm to, information systems and internet connected devices (to include hardware, software and associated infrastructure), the data on them and the services they provide, primarily by cyber means.

**Data Breach –** the unauthorised movement or disclosure of information on a network to a party who is not authorised to have access to, or see, the information.

**Domain –** a domain name locates an organisation or other entity on the Internet and corresponds to an Internet Protocol (IP) address.

**Devolved government or devolved administration –** The separate legislatures and executives in Scotland, Wales and Northern Ireland following devolution, responsible for many domestic policy issues with the power to make laws for these areas.

**Digital Twin –** a virtual replica or representation of assets, processes, systems, or institutions in the built, societal, or natural environments that provides insight into how complex physical assets and citizens behave, helping organisations improve decision-making and optimise processes. Changes in the real world are reflected in the twin, and changes in the twin can be replicated automatically in the real world.

**Five Eyes –** Five Eyes is the name of the intelligence alliance between the USA, UK, Canada, Australia and New Zealand which helps share information to keep its citizens as safe as possible from threats.

**GCHQ –** Government Communications Headquarters; the centre for the Government's signals intelligence activities and Cyber National Technical Authority (NTA).

**GFCE –** Global Forum on Cyber Expertise.

**Government Cyber Coordination Centre (GCCC) –** Proposed joint venture between GSG, CDDO and NCSC bringing together their respective functions and areas of expertise to better coordinate operational cyber security efforts across government, transform how cyber security data and threat intelligence is used across government and truly enhance government's ability to 'defend as one'.

**Horizon-scanning –** a systematic examination of information to identify potential threats, risks, emerging issues and opportunities allowing for better preparedness and the incorporation of mitigation and exploitation into the policy-making process.

**ICANN –** Internet Corporation for Assigned Names and Numbers. It coordinates website names and IP addresses.

**Incident Management –** the management and coordination of activities to investigate, and remediate, an actual or potential occurrence of an adverse cyber event that may compromise or cause harm to a system or network.

**Incident Response –** the activities that address the short-term, direct effects of an incident, and may also support short-term recovery.

**Industrial Control System (ICS) –** an information system used to control industrial processes, such as manufacturing, product handling, production and distribution, or to control infrastructure assets.

**Integrated Review –** 'Global Britain in a Competitive Age, the Integrated Review of Security, Defence, Development and Foreign Policy', describes the government's vision for the UK's role in the world over the next decade and the action government will take to 2025.

**Integrity –** in information security, integrity means that information has not been changed accidentally, or deliberately, and is accurate and complete.

**Internet –** a global computer network, providing a variety of information and communication facilities, consisting of interconnected networks using standardised communication protocols.

**Internet of Things –** the totality of devices, vehicles, buildings and other items embedded with electronics, software and sensors that communicate and exchange data over the Internet.

**Legacy IT –** Legacy IT refers to systems and their component software and hardware that are outside of vendor support, on extended support and/or on bespoke support arrangements

**Managed Service Providers –** third parties that provide a set of defined services to a customer and assume the responsibility of running, maintaining, and securing those services.

**Microgeneration –** the small-scale generation of energy by households, small businesses and communities.

**NATO –** North Atlantic Treaty Organisation.

**NCA –** National Crime Agency.

**National Cyber Security Centre (NCSC) –** the UK's technical authority for cyber threats, providing a unified national response to cyber incidents to minimise harm, helping with recovery and learning lessons for the future.

**Network and Information Systems (NIS) Regulations 2018 –** UK regulations that provide legal measures to boost the level of security (both cyber & physical resilience) of network and information systems for the provision of essential services and digital services.

**OECD –** The Organisation for Economic Co-operation and Development, an intergovernmental economic organisation.

**Offensive Cyber –** adding, deleting or manipulating data on systems or networks to deliver a physical, virtual or cognitive effect. Offensive cyber operations often exploit technical vulnerabilities, use systems or networks in ways that their owners and operators would not intend or condone, and may rely on deception or misrepresentation.

**Operational Technologies (OT) –** combine hardware and software to monitor, control and automate physical processes, particularly in industrial sectors such as energy, manufacturing, water, and transport.

**Operators of Essential Services –** organisations within vital sectors which rely heavily on information networks, for example utilities, healthcare, transport, and digital infrastructure sectors as identified by the criteria in the Network and Information Systems (NIS) Regulations 2018.

**Plan for Digital Regulation –** sets out the government's overall approach for governing digital technologies in order to drive growth and innovation.

**Quantum Technologies –** Quantum technology relies on the principles of quantum physics. The advancing understanding and control of what are known as 'quantum effects' such as superposition and entanglement will lead to a new wave of advances that will underpin our economy and society: sensing, data transmission and encryption, timing and computing.

**Ransomware –** malicious software that denies the user access to their files, computer or device until a ransom is paid.

**Secure by Design –** software, hardware and systems that have been designed from the ground up to be secure.

**Vulnerability –** bugs in software programs that have the potential to be exploited by attackers.

**Vulnerability Reporting Service –** A mechanism through which an organisation can be alerted to security flaws before they are exploited by attackers.