HM Government

NATIONAL CYBER SECURITY STRATEGY 2016-2021

Contents

FOREWORD

The UK is one of the world's leading digital nations. Much of our prosperity now depends on our ability to secure our technology, data and networks from the many threats we face.

Yet cyber attacks are growing more frequent, sophisticated and damaging when they succeed. So we are taking decisive action to protect both our economy and the privacy of UK citizens.

Our National Cyber Security Strategy sets out our plan to make Britain confident, capable and resilient in a fast-moving digital world.

Over the lifetime of this five-year strategy, we will invest £1.9 billion in defending our systems and infrastructure, deterring our adversaries, and developing a whole-society capability – from the biggest companies to the individual citizen.

From the most basic cyber hygiene, to the most sophisticated deterrence, we need a comprehensive response.

We will focus on raising the cost of mounting an attack against anyone in the UK, both through stronger defences and better cyber skills. This is no longer just an issue for the IT department but for the whole workforce. Cyber skills need to reach into every profession.

The new National Cyber Security Centre will provide a hub of world-class, user-friendly expertise for businesses and individuals, as well as rapid response to major incidents.

Government has a clear leadership role, but we will also foster a wider commercial ecosystem, recognising where industry can innovate faster than us. This includes a drive to get the best young minds into cyber security.

The cyber threat impacts the whole of our society, so we want to make very clear that everyone has a part to play in our national response. It's why this strategy is an unprecedented exercise in transparency. We can no longer afford to have this discussion behind closed doors.

Ultimately, this is a threat that cannot be completely eliminated. Digital technology works because it is open, and that openness brings with it risk. What we can do is reduce the threat to a level that ensures we remain at the vanguard of the digital revolution. This strategy sets out how.

The Rt Hon Philip Hammond MP, Chancellor of the Exchequer

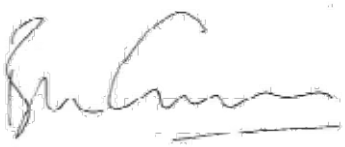
PREFACE

Our primary responsibility is to keep the nation safe and deliver competent government. This strategy reflects these duties. It is a bold and ambitious approach to tackling the many threats our country faces in cyberspace. Managing and mitigating those threats is a task for us all but the Government recognises its special responsibility to lead the national effort required.

The Government is committed to ensuring the commitments set out in this strategy are carried out and that we accurately monitor and regularly report on progress in meeting them. We will also keep our approach under review and respond to changes in the level of threat we face as well as evolutions in security technologies.

Government also has a special responsibility to the citizen, to companies and organisations operating in the UK, and to our international allies and partners. We should be able to assure them that every effort made has been to render our systems safe and to protect our data and our networks from attack or interference. We must therefore set ourselves the highest standards of cyber security and ensure we adhere to them, both as the cornerstone of the country's national security and economic wellbeing and also as an example for others to follow. We shall report back on progress made on an annual basis.

As Minister for the Cabinet Office with responsibility for cyber security and government security, I am determined to see this strategy implemented in full. I will work closely with colleagues across Government and with partners in the Devolved Administrations, the wider public sector, industry and academia to ensure we achieve that ambition.



The Rt Hon Ben Gummer MP,
Minister for the Cabinet Office
and Paymaster General

1. EXECUTIVE SUMMARY

1.1. The future of the UK's security and prosperity rests on digital foundations. The challenge of our generation is to build a flourishing digital society that is both resilient to cyber threats, and equipped with the knowledge and capabilities required to maximise opportunities and manage risks.

1.2. We are critically dependent on the Internet. However, it is inherently insecure and there will always be attempts to exploit weaknesses to launch cyber attacks. This threat cannot be eliminated completely, but the risk can be greatly reduced to a level that allows society to continue to prosper, and benefit from the huge opportunities that digital technology brings.

1.3. The 2011 National Cyber Security Strategy, underpinned by the British Government's £860m National Cyber Security Programme, has delivered substantial improvements to UK cyber security. It achieved important outcomes by looking to the market to drive secure cyber behaviours. But this approach has not achieved the scale and pace of change required to stay ahead of the fast moving threat. We now need to go further.

1.4. Our vision for 2021 is that **the UK is secure and resilient to cyber threats, prosperous and confident in the digital world.**

1.5. To realise this vision we will work to achieve the following objectives:

- **DEFEND** We have the means to defend the UK against evolving cyber threats, to respond effectively to incidents, to ensure UK networks, data and systems are protected and resilient. Citizens, businesses and the public sector have the knowledge and ability to defend themselves.

- **DETER** The UK will be a hard target for all forms of aggression in cyberspace. We detect, understand, investigate and disrupt hostile action taken against us, pursuing and prosecuting offenders. We have the means to take offensive action in cyberspace, should we choose to do so.

- **DEVELOP** We have an innovative, growing cyber security industry, underpinned by world-leading scientific research and development. We have a self-sustaining pipeline of talent providing the skills to meet our national needs across the public and private sectors. Our cutting-edge analysis and expertise will enable the UK to meet and overcome future threats and challenges.

1.6. Underpinning these objectives, we will pursue **INTERNATIONAL ACTION** and exert our influence by investing in partnerships that shape the global evolution of cyberspace in a manner that advances our wider economic and security interests. We will deepen existing links with our closest international partners, recognising that this enhances our collective security. We will also develop relationships with new partners to build their levels of cyber security and protect UK interests overseas. We will do this both bilaterally and multilaterally, including through the EU, NATO and the UN. We will deliver clear messages about consequences to adversaries who threaten to harm our interests, or those of our allies, in cyberspace.

1.7. To achieve these outcomes over the next five years, the UK Government intends to intervene more actively and use increased investment, while continuing

to support market forces to raise cyber security standards across the UK. The UK Government, in partnership with the Devolved Administrations of Scotland, Wales and Northern Ireland, will work with the private and public sectors to ensure that individuals, businesses and organisations adopt the behaviours required to stay safe on the Internet. We will have measures in place to intervene (where necessary and within the scope of our powers) to drive improvements that are in the national interest, particularly in relation to the cyber security of our critical national infrastructure.

1.8. The UK Government will draw on its capabilities and those of industry to develop and apply active cyber defence measures to significantly enhance the levels of cyber security across UK networks. These measures include minimising the most common forms of phishing attacks, filtering known bad IP addresses, and actively blocking malicious online activity. Improvements in basic cyber security will raise the UK's resilience to the most commonly deployed cyber threats.

1.9. We have created a National Cyber Security Centre (NCSC) to be the authority on the UK's cyber security environment, sharing knowledge, addressing systemic vulnerabilties and providing leadership on key national cyber security issues.

1.10. We will ensure that our Armed Forces are resilient and have the strong cyber defences they need to secure and defend their networks and platforms, continuing to operate and retaining global freedom of manoeuvre despite cyber threats. Our military Cyber Security Operations Centre will work closely with the NCSC and we will ensure that the Armed Forces can assist in the event of a significant national cyber attack.

1.11. We will have the means to respond to cyber attacks in the same way as we respond to any other attack, using whichever capability is most appropriate, including an offensive cyber capability.

1.12. We will use the authority and influence of the UK Government to invest in programmes to address the shortage of cyber security skills in the UK, from schools to universities and across the workforce.

1.13. We will launch two new cyber innovation centres to drive the development of cutting-edge cyber products and dynamic new cyber security companies. We will also allocate a proportion of the £165m Defence and Cyber Innovation Fund to support innovative procurement in defence and security.

1.14. We will invest a total of £1.9 billion over the next five years to transform significantly the UK's cyber security.

[1] Understanding the threats to networks, and then devising and implementing measures to proactively combat or defend against those threats. See Glossary for an explanation of all technical terms.

2. INTRODUCTION

2.1. Information and communication technologies have evolved over the last two decades and are now integrated into virtually every aspect of our lives. The UK is a digitalised society. Our economy and our daily lives are the richer for it.

2.2. The transformation brought about by this digitalisation creates new dependencies. Our economy, the administration of government and the provision of essential services now rely on the integrity of cyberspace and on the infrastructure, systems and data which underpin it. A loss of trust in that integrity would jeopardise the benefits of this technological revolution.

2.3. Much of the hardware and software originally developed to facilitate this interconnected digital environment has prioritised efficiency, cost and the convenience of the user, but has not always had security designed in from the start. Malicious actors – hostile states, criminal or terrorist organisations and individuals – can exploit the gap between convenience and security. Narrowing that gap is a national priority.

2.4. The expansion of the Internet beyond computers and mobile phones into other cyber-physical or 'smart' systems is extending the threat of remote exploitation to a whole host of new technologies. Systems and technologies that underpin our daily lives – such as power grids, air traffic control systems, satellites, medical technologies, industrial plants and traffic lights – are connected to the Internet and, therefore, potentially vulnerable to interference.

2.5. The 2015 National Security Strategy (NSS) reaffirmed the cyber threat as a Tier One risk to UK interests. The NSS set out the Government's determination to address cyber threats and "put in place tough and innovative measures, as a world leader in cyber security". This National Cyber Security Strategy delivers on that commitment.

2.6. In preparing this new strategy, the Government is building on the achievements, objectives and judgements of the first five-year National Cyber Security Strategy issued in 2011. The Government invested £860m over that period, and is proud of what has been achieved. The policies, institutions and initiatives developed over the last five years have helped to establish the UK as a leading global player in cyber security.

2.7. These are sound foundations. But the persistence and ingenuity of those who would threaten us, the prevalence of our vulnerabilities and gaps in our capabilities and defences mean we need to work even harder to keep pace with the threat. A comprehensive approach is required if we are to effectively secure our cyber interests. Our resolution to make further investment and interventions is based on the following assessments:

- the scale and dynamic nature of cyber threats, and our vulnerability and dependency, mean that maintaining the current approach will not in itself be sufficient to keep us safe;
- a market based approach to the promotion of cyber hygiene has not produced the required pace and scale of change; therefore, Government has to lead the way and intervene more directly by bringing its influence and resources to bear to address cyber threats;
- the Government alone cannot provide for all aspects of the nation's cyber security. An embedded and sustainable approach is needed

where citizens, industry and other partners in society and government, play their full part in securing our networks, services and data;
- the UK needs a vibrant cyber security sector and supporting skills base that can keep pace with and get ahead of the changing threat.

THE SCOPE OF THE STRATEGY

2.8. This strategy is intended to shape the Government's policy, while also offering a coherent and compelling vision to share with the public and private sector, civil society, academia and the wider population.

2.9. The strategy covers the whole of the UK. The UK Government will seek to ensure the strategy is implemented for all parts of the UK, recognising that, to the extent that it touches on devolved matters, we will work closely with the devolved Governments on its application to Scotland, Wales and Northern Ireland (respecting the three separate legal jurisdictions, and four education systems, that exist in the UK). Where proposals set out in the strategy relate to devolved matters, their implementation will be agreed as appropriate with those Governments in accordance with the devolution settlements.

2.10. The strategy sets out proposed or recommended actions aimed at all sectors of the economy and society, from central government departments, to leaders across industry and the individual citizen. The strategy aims to increase

cyber security at all levels for our collective benefit and will be the basis on which the UK engages internationally to promote good internet governance.

2.11. In this strategy, 'cyber security' refers to the protection of information systems (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.

2.12. Consistent with our assessment of the challenge we face and building on the achievements of the 2011 strategy, this document sets out:

- our updated assessment of the strategic context, including the current and evolving threats: who poses the most serious threat to our interests, and the tools at their disposal;
- a review of vulnerabilities and how these have developed over the last five years;
- the Government's vision for cyber security in 2021 and the key objectives to achieve that goal, including guiding principles, roles and responsibilities, and how and where government intervention will make a difference;
- how we intend to put our policy into practice: setting out where the Government will lead and where we expect to work in partnership with others; and
- how we intend to assess our progress towards our objectives.

3. STRATEGIC CONTEXT

3.1. When the last National Cyber Security Strategy was published in 2011, the scale of technological change and its impact was already apparent. The trends and opportunities described then have since accelerated. New technologies and applications have come to the fore, and greater uptake of internet-based technologies worldwide, in particular in developing countries, has offered increasing opportunities for economic and social development. These developments have brought, or will bring, significant advantages to connected societies such as ours. But as our reliance on networks in the UK and overseas grows, so do the opportunities for those who would seek to compromise our systems and data. Equally, the geopolitical landscape has changed. Malicious cyber activity knows no international boundaries. State actors are experimenting with offensive cyber capabilities. Cyber criminals are broadening their efforts and expanding their strategic modus operandi to achieve higher value pay-outs from UK citizens, organisations and institutions. Terrorists, and their sympathisers, are conducting low-level attacks and aspire to carry out more significant acts. This chapter sets out our assessment of the nature of these threats, our vulnerabilities and how these continue to evolve.

THREATS

Cyber criminals

3.2. This strategy deals with cyber crime in the context of two interrelated forms of criminal activity:

- cyber-dependent crimes – crimes that can be committed only through the use of Information and Communications Technology (ICT) devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity); and
- cyber-enabled crimes – traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft).

3.3. Much of the most serious cyber crime – mainly fraud, theft and extortion – against the UK continues to be perpetrated predominantly by financially motivated Russian-language organised criminal groups (OCGs) in Eastern Europe, with many of the criminal marketplace services being hosted in these countries. However, the threat also emanates from other countries and regions, and from inside the UK itself, with emerging threats from South Asia and West Africa of increasing concern.

3.4. Even when key individuals responsible for the most damaging cyber criminal activities against the UK are identified, it is often difficult for the UK and international law enforcement agencies to prosecute them when they are located in jurisdictions with limited, or no, extradition arrangements.

3.5. These OCGs are principally responsible for developing and deploying the increasingly advanced malware that infects the computers and networks of UK citizens, our industry and government. The impact is dispersed throughout the UK, but the cumulative effect is significant. These attacks are becoming increasingly aggressive and confrontational, as illustrated by the increasing use of ransomware, and threats of distributed denial of service (DDoS) for extortion.

3.6. Whilst OCGs may pose a significant threat to our collective prosperity and security, equally of concern is the continuing threat from acts of less sophisticated but widespread cyber crimes carried out against individuals or smaller organisations.

Internet banking fraud, which covers fraudulent payments taken from a customer's bank account using the internet banking channel, rose by 64% to £133.5m in 2015. The number of cases increased at a lower rate of 23%, which Financial Fraud Action UK said is evidence of the growing trend for criminals to target business and high-net-worth customers.

States and state-sponsored threats

3.7. We regularly see attempts by states and state-sponsored groups to penetrate UK networks for political, diplomatic, technological, commercial and strategic advantage, with a principal focus on the government, defence, finance, energy and telecommunications sectors.

3.8. The capacity and impact of these state cyber programmes varies. The most advanced nations continue to improve their capabilities at pace, integrating encryption and anonymisation services into their tools in order to remain covert. While they have the technical capability to deploy sophisticated attacks, they can often achieve their aims using basic tools and techniques against vulnerable targets because the defences of their victims are poor.

3.9. Only a handful of states have the technical capabilities to pose a serious threat to the UK's overall security and prosperity. But many other states are developing sophisticated cyber programmes that could pose a threat to UK interests in the near future. Many states seeking to develop cyber espionage capability can purchase computer network exploitation tools 'off the shelf' and repurpose these to conduct espionage.

3.10. Beyond the espionage threat, a small number of hostile foreign threat actors have developed and deployed offensive cyber capabilities, including destructive ones. These capabilities threaten the security of the UK's critical national infrastructure and industrial control systems. Some states may use these capabilities in contravention of international law in the belief that they can do so with relative impunity, encouraging others to follow suit. Whilst destructive attacks around the world remain rare, they are rising in number and impact.

Terrorists

3.11. Terrorist groups continue to aspire to conduct damaging cyber activity against the UK and its interests. The current technical capability of terrorists is judged to be low. Nonetheless the impact of even low-capability activity against the UK to date has been disproportionately high: simple defacements and doxing activity (where hacked personal details are 'leaked' online) enable terrorist groups and their supporters to attract media attention and intimidate their victims.

> "Terrorists using the Internet for their purposes does not equal cyber-terrorism. However, by increasingly engaging in cyber-space, and given the availability of cyber-crime as a service, one can assume that they would be in the position to launch cyber attacks"
>
> ENISA Threat Landscape 2015

3.12. The current assessment is that physical, rather than cyber, terrorist attacks will remain the priority for terrorist groups for the immediate future. As an increasingly computer-literate generation engages in extremism, potentially exchanging enhanced technical skills, we envisage a greater volume of low-sophistication (defacement or DDoS) disruptive activity against the UK. The potential for a number of skilled extremist lone actors to emerge will also increase, as will the risk that a terrorist organisation will seek to enlist an established insider. Terrorists will likely use any cyber capability to achieve the maximum effect possible. Thus, even a moderate increase in terrorist capability may constitute a significant threat to the UK and its interests.

Hacktivists

3.13. Hacktivist groups are decentralised and issue-orientated. They form and select their targets in response to perceived grievances, introducing a vigilante quality to many of their acts. While the majority of hacktivist cyber activity is disruptive in nature (website defacement or DDoS), more able hacktivists have been able to inflict greater and lasting damage on their victims.

INSIDERS

Insider threats remain a cyber risk to organisations in the UK. Malicious insiders, who are trusted employees of an organisation and have access to critical systems and data, pose the greatest threat. They can cause financial and reputational damage through the theft of sensitive data and intellectual property. They can also pose a destructive cyber threat if they use their privileged knowledge, or access, to facilitate, or launch, an attack to disrupt or degrade critical services on the network of their organisations, or wipe data from the network.

Of equal concern are those insiders or employees who accidentally cause cyber harm through inadvertent clicking on a phishing email, plugging an infected USB into a computer, or ignoring security procedures and downloading unsafe content from the Internet. Whilst they have no intention of deliberately harming the organisation, their privileged access to systems and data mean their actions can cause just as much damage as a malicious insider. These individuals are often the victims of social engineering – they can unwittingly provide access to the networks of their organisation or carry out instructions in good faith that benefit the fraudster.

The overall cyber risk to an organisation from insider threats is not just about unauthorised access to information systems and their content. The physical security controls protecting those systems from inappropriate access, or removal of sensitive data or proprietary information on different forms of media, are equally important. Similarly, a robust personnel security culture that is alive to the threat posed by disaffected employees, fraud in the workforce and industrial and other forms of espionage is an important element in a comprehensive approach to security.

'Script Kiddies'

3.14. So-called 'script kiddies' – generally less skilled individuals who use scripts or programmes developed by others to conduct cyber attacks – are not assessed as posing a substantive threat to the wider economy or society. But they do have access to hacking guides, resources and tools on the Internet. Due to the vulnerabilities found in internet-facing systems used by many organisations, the actions of 'script kiddies' can, in some cases, have a disproportionately damaging impact on an affected organisation.

CASE STUDY 1: TALKTALK COMPROMISE

On 21 October 2015, UK telecommunications provider TalkTalk reported a successful cyber attack and a possible breach of customer data. Subsequent investigation determined that a database containing customer details had been accessed via public-facing internet servers, with the records of approximately 157,000 customers at risk, including names, addresses and bank account details.

On the same day, several TalkTalk employees received an email with a ransom demand for payment in Bitcoins. The attackers detailed the structure of the database as apparent proof that it had been accessed.

TalkTalk's report of the breach helped the police, supported by specialists at the National Crime Agency, to arrest the main suspects, all based in the UK, in October and November 2015.

The attack demonstrates that, even within large cyber-aware organisations, vulnerabilities can persist. Their exploitation can have a disproportionate effect in terms of reputational damage and operational disruption, and this incident generated substantial media attention. TalkTalk's rapid reporting of the breach enabled law enforcement to respond in a timely manner, and both the public and government to mitigate the potential loss of sensitive data. The incident cost TalkTalk an estimated £60m and the loss of 95,000 customers, as well as a sharp drop in their share price.

CASE STUDY 2: ATTACK ON BANGLADESH BANK'S SWIFT SYSTEM

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) provides a network that enables financial institutions worldwide to send and receive information about financial transactions in a secure way. As SWIFT sends payment orders which must be settled by correspondent accounts that the institutions have with each other, there has long been concern over any potential for this process to be compromised by cyber criminals or other malicious actors, seeking to inject illegitimate payment orders into the system or, in a worst case scenario, seeking to disable or disrupt the functionality of the SWIFT network itself.

In early February 2016, an attacker accessed the SWIFT payment system of the Bangladesh Bank and instructed the New York Federal Reserve bank to transfer money from Bangladesh Bank's account to accounts in the Philippines. The attempted fraud was US$951 million. 30 transactions, worth US$850 million, were prevented by the banking system; however, five transactions worth US$101 million went through. US$20 million, traced to Sri Lanka, has since been recovered. The remaining US$81 million transferred to the Philippines was laundered through casinos and some of the funds were then forwarded to Hong Kong.

The forensic investigation launched by Bangladesh Bank discovered that malware had been installed on the bank's systems and had been used to gather intelligence on the procedures used by the bank for international payments and fund transfers. Further analysis by BAE Systems of the malware linked to the attack uncovered sophisticated functionality for interacting with the local SWIFT Alliance Access software running in the Bangladesh Bank infrastructure. BAE concluded 'that criminals are conducting more and more sophisticated attacks against victim organisations, particularly in the area of network intrusions'.

CASE STUDY 3: UKRAINE POWER GRID ATTACK

A cyber attack on western Ukrainian electricity distribution companies Prykarpattya Oblenergo and Kyiv Oblenergo on 23 December 2015 caused a major power outage, with disruption to over 50 substations on the distribution networks. The region reportedly experienced a blackout for several hours and many other customers and areas sustained lesser disruptions to their power supplies, affecting more than 220,000 consumers.

Use of the BlackEnergy3 malware has been blamed by some for the attack, after samples were identified on the network. At least six months before the attack, attackers had sent phishing emails to the offices of power utility companies in the Ukraine containing malicious Microsoft Office documents. However, the malware was not likely to have been responsible for opening the circuit breakers which resulted in the outage. It is probable that the malware enabled the attackers to gather credentials that allowed them to gain direct remote control of aspects of the network, which would subsequently enable them to trigger the outage.

This Ukraine incident is the first confirmed instance of a disruptive cyber attack on an electricity network. Instances such as this further demonstrate the need for good cyber security practices across all of our Critical National Infrastructure (CNI) to prevent similar incidents occurring in the UK.

VULNERABILITIES

An expanding range of devices

3.15. When the last National Cyber Security Strategy was published in 2011, most people conceived of cyber security through the prism of protecting devices such as their desktop computer or laptop. Since then the Internet has become increasingly integrated into our daily lives in ways we are largely oblivious to. The 'Internet of Things' creates new opportunities for exploitation and increases the potential impact of attacks which have the potential to cause physical damage, injury to persons and, in a worst case scenario, death.

3.16. The rapid implementation of connectivity in industrial control processes in critical systems, across a wide range of industries such as energy, mining, agriculture and aviation, has created the Industrial Internet of Things. This is simultaneously opening up the possibility of devices and processes, which were never vulnerable to such interference in the past, being hacked and tampered with, with potentially disastrous consequences.

3.17. Therefore, we are no longer just vulnerable to cyber harms caused by the lack of cyber security on our own devices but by threats to the interconnected systems that are fundamental to our society, health and welfare.

Poor cyber hygiene and compliance

3.18. Awareness of technical vulnerabilities in software and networks, and the need for cyber hygiene in the UK, has undoubtedly increased over the past five years. This is in part a consequence of initiatives like the Government's '10 Steps to Cyber Security', but also due to the increased public profile of major cyber incidents affecting governments and corporations. Cyber attacks are not necessarily sophisticated or inevitable and are often the result of exploited – but easily rectifiable and, often, preventable – vulnerabilities. In most cases, it continues to be the vulnerability of the victim, rather than the ingenuity of the attacker, that is the deciding factor in the success of a cyber attack. Businesses and organisations decide on where and how to invest in cyber security based on a cost-benefit assessment, but they are ultimately liable for the security of their data and systems. Only by balancing the risk to their critical systems and sensitive data from cyber attacks, with sufficient investment in people, technology and governance, will businesses reduce their exposure to potential cyber harm.

> "There is no conceivable information security system that can stop one person out of a hundred opening a phishing email, and that can be all it takes."
>
> Ciaran Martin, Director General for Cyber Security, GCHQ – June 2015

Insufficient training and skills

3.19. We lack the skills and knowledge to meet our cyber security needs across both the public and private sector. In businesses, many staff members are not cyber security aware and do not understand their responsibilities in this regard, partially due to a lack of formal training. The public is also insufficiently cyber aware.

"Just under a fifth of businesses had their staff take part in cyber security training in the past year."

Cyber Security Breaches Survey 2016.

3.20. We also need to develop the specialist skills and capabilities that will allow us to keep pace with rapidly evolving technology and manage the associated cyber risks. This skills gap represents a national vulnerability that must be resolved.

Legacy and unpatched systems

3.21. Many organisations in the UK will continue to use vulnerable legacy systems until their next IT upgrade. Software on these systems will often rely on older, unpatched versions. These older versions often suffer from vulnerabilities that attackers look for and have the tools to exploit. An additional issue is the use by some organisations of unsupported software, for which patching regimes do not exist.

"We recently analysed 115,000 Cisco devices on the Internet and across customer environments as a way to bring attention to the security risks that aging infrastructure – and lack of attention to patching vulnerabilities present… We found that 106,000 of the 115,000 devices had known vulnerabilities in the software they were running."

Cisco 2016 Annual Security Report

Availability of hacking resources

3.22. The ready availability of hacking information and user-friendly hacking tools on the Internet is enabling those who want to develop a hacking capability to do so. The information hackers need in order to compromise victims successfully is often openly accessible and can be harvested quickly. Everyone, from the living room to the boardroom, needs to be aware of the extent of exposure of their personal details and systems on the Internet, and the degree to which that could leave them vulnerable to malicious cyber exploitation.

"99.9% of exploited vulnerabilities were compromised more than a year after the vulnerability was published."

Verizon 2015 Data Breach Investigations report

CONCLUSIONS

3.23. The UK has pursued policies and established institutions that have enhanced our defences and mitigated some of the threat we face in cyberspace.

3.24. However, we are not yet ahead of the threat. The types of malicious cyber actors we must contend with, and their motivations, have largely endured, even as the volume of malware and the numbers of such malicious actors has grown rapidly. The capability of our most technically proficient adversaries, namely a select number of states and elite cyber criminals, has grown. Our collective challenge is to ensure our defences are evolved and agile enough to counter them, to reduce the ability of malicious actors to attack us and to address the root causes of the vulnerabilities outlined above.

4. OUR NATIONAL RESPONSE

4.1. To mitigate the multiple threats we face and safeguard our interests in cyberspace, we need a strategic approach that underpins all our collective and individual actions in the digital domain over the next five years. This section sets out our vision and strategic approach.

OUR VISION

4.2. Our vision for 2021 is that **the UK is secure and resilient to cyber threats, prosperous and confident in the digital world.**

4.3. To realise this vision, we will work to achieve the following objectives:

- **DEFEND** We have the means to defend the UK against evolving cyber threats, to respond effectively to incidents, and to ensure UK networks, data and systems are protected and resilient. Citizens, businesses and the public sector have the knowledge and ability to defend themselves.

- **DETER** The UK will be a hard target for all forms of aggression in cyberspace. We detect, understand, investigate and disrupt hostile action taken against us, pursuing and prosecuting offenders. We have the means to take offensive action in cyberspace, should we choose to do so.

- **DEVELOP** We have an innovative, growing cyber security industry, underpinned by world-leading scientific research and development. We have a self-sustaining pipeline of talent providing the skills to meet our national needs across the public and private sectors. Our cutting-edge analysis and expertise will enable the UK to meet and overcome future threats and challenges.

4.4. Underpinning these objectives, we will pursue **INTERNATIONAL ACTION** and exert our influence by investing in partnerships. We will shape the global evolution of cyberspace in a manner that advances our wider economic and security interests.

PRINCIPLES

4.5 In working towards these objectives, the Government will apply the following principles:

- our actions and policies will be driven by the need to both protect our people and enhance our prosperity;
- we will treat a cyber attack on the UK as seriously as we would an equivalent conventional attack and we will defend ourselves as necessary;
- we will act in accordance with national and international law and expect others to do the same;
- we will rigorously protect and promote our core values. These include democracy; the rule of law; liberty; open and accountable governments and institutions; human rights; and freedom of expression;
- we will preserve and protect UK citizens' privacy;
- we will work in partnership. Only by working with the Devolved Administrations, all parts of the public sector, businesses, institutions, and the individual citizen, can we successfully secure the UK in cyberspace;
- the Government will meet its responsibilities and lead the national response, but businesses, organisations and individual citizens

have a responsibility to take reasonable steps to protect themselves online and ensure they are resilient and able to continue operating in the event of an incident;
- responsibility for the security of organisations across the public sector, including cyber security and the protection of online data and services, lies with respective Ministers, Permanent Secretaries and Management Boards;
- we will not accept significant risk being posed to the public and the country as a whole as a result of businesses and organisations failing to take the steps needed to manage cyber threats;
- we will work closely with those countries that share our views and with whom our security overlaps, recognising that cyber threats know no borders. We will also work broadly across the range of international partners to influence the wider community, acknowledging the value of broad coalitions; and
- to ensure Government interventions are having a substantive impact on overall national cyber security and resilience, we will seek to define, analyse and present data which measures the state of our collective cyber security and our success in meeting our strategic goals.

ROLES AND RESPONSIBILITIES

4.6. Securing the national cyberspace will require a collective effort. Each and every one of us has an important part to play.

Individuals

4.7. As citizens, employees and consumers, we take practical steps to secure the assets we value in the physical world. In the virtual world, we must do the same. That means fulfilling our personal responsibility to take all reasonable steps to safeguard not only our hardware – our smart phones and other devices – but also the data, software and systems that afford us freedom, flexibility and convenience in our private and professional lives.

Businesses and organisations

4.8. Businesses, public and private sector organisations and other institutions hold personal data, provide services, and operate systems in the digital domain. The connectivity of this information has revolutionised their operations. But with this technological transformation comes the responsibility to safeguard the assets which they hold, maintain the services they provide, and incorporate the appropriate level of security into the products they sell. The citizen and consumer, and society at large, look to businesses and organisations to take all reasonable steps to protect their personal data, and build resilience – the ability to withstand and recover – into the systems and structures on which they depend. Businesses and organisations must also understand that, if they are the victim of a cyber attack, they are liable for the consequences.

Government

4.9. The primary duty of the Government is to defend the country from attacks by other states, to protect citizens and the economy from harm, and to set the domestic and international framework to protect our interests, safeguard fundamental rights, and bring criminals to justice.

4.10. As the holder of significant data and a provider of services, the Government takes stringent measures to provide safeguards for its information assets. The Government also has an important responsibility to advise and inform citizens

and organisations what they need to do to protect themselves online, and where necessary, set the standards we expect key companies and organisations to meet.

4.11. Although key sectors of our economy are in private hands, the Government is ultimately responsible for assuring their national resilience and, with its partners across the administration, the maintenance of essential services and functions across the whole of government.

Driving change: the role of the market

4.12. The 2011 Strategy and National Cyber Security Programme sought to drive outcomes and increase capacity in both the public and private sector by looking to the market to drive the right behaviours. We expected commercial pressures and government-instigated incentives to ensure adequate business investment in appropriate cyber security, to stimulate a flow of investment into our industry, and to encourage an adequate pipeline of skills into the sector.

4.13. Much has been achieved. Across the economy and wider society, awareness of the risk and of the actions required to mitigate cyber risk have increased over the last five years. But the combination of market forces and government encouragement has not been sufficient in itself to secure our long-term interests in cyberspace at the pace required. Too many networks, including in critical sectors, are still insecure. The market is not valuing, and therefore not managing, cyber risk correctly. Too many organisations are still suffering breaches at even the most basic level. Too few investors are willing to risk supporting entrepreneurs in the sector. Too few graduates and others with the right skills are emerging from the education and training system.

4.14. The market still has a role to play and in the longer term will deliver greater impact than the Government ever can. However, the immediacy of the threat facing the UK and the expanding vulnerabilities of our digitalised environment call for greater action in the short term from the Government.

Driving change: expanded role for the Government

4.15. The Government must therefore set the pace in meeting the country's national cyber security needs. Only Government can draw on the intelligence and other assets required to defend the country from the most sophisticated threats. Only Government can drive cooperation across the public and private sectors and ensure information is shared between the two. Government has a leading role, in consultation with industry, in defining what good cyber security looks like and ensuring it is implemented.

4.16. The Government will bring about a significant improvement in our national cyber security over the next five years. This ambitious and transformational programme will focus on the following four broad areas:

- **Levers and incentives**. The Government will invest to maximise the potential of a truly innovative UK cyber sector. We will do this by supporting start-ups and investing in innovation. We will also seek to identify and bring on talent earlier in the education system and develop clearer routes into a profession that needs better definition. The Government will also make use of all available levers, including the forthcoming General Data Protection Regulation (GDPR), to drive up standards of cyber security across the economy, including, if required, through regulation.

- **Expanded intelligence and law enforcement focus on the threat**. The intelligence agencies, the Ministry of Defence, the police and the National Crime Agency, in coordination with international partner agencies, will expand their efforts to identify, anticipate and disrupt hostile cyber activities by foreign actors, cyber criminals and terrorists. This will improve their intelligence collection and exploitation, with the aim of obtaining pre-emptive intelligence on the intent and capabilities of our adversaries.
- **Development and deployment of technology** in partnership with industry, including Active Cyber Defence measures, to deepen our understanding of the threat, to strengthen the security of the UK public and private sector systems and networks in the face of that threat, and to disrupt malicious activity.
- **National Cyber Security Centre (NCSC)**. The Government has established a single, central body for cyber security at a national level. This body will manage national cyber incidents, provide an authoritative voice and centre of expertise on cyber security, and deliver tailored support and advice to departments, the Devolved Administrations, regulators and businesses. The NCSC will analyse, detect and understand cyber threats, and will also provide its cyber security expertise to support the Government's efforts to foster innovation, support a thriving cyber security industry, and stimulate the development of cyber security skills. Uniquely for such a public-facing body, its parent body is GCHQ and it can therefore draw on the world-class expertise and sensitive capabilities of that organisation, improving the support it will be able to provide to the economy and society more widely. It will remain the responsibility of government departments to ensure they effectively implement this cyber security advice.

"Given the industrial-scale theft of intellectual property from our companies and universities, as well as the numerous phishing and malware scams that waste time and money, the National Cyber Security Centre shows that the UK is focusing its efforts to combat the threats that exist online."

Robert Hannigan, Director GCHQ, March 2016

4.17. Delivering these changes to our cyber security and resilience will require additional resources. In the Strategic Defence and Security Review 2015, the Government set aside £1.9 billion over the five years of the strategy to deliver these commitments and objectives.

THE NATIONAL CYBER SECURITY CENTRE

The National Cyber Security Centre (NCSC) launched on 1 October 2016. The NCSC provides a unique opportunity to build effective cyber security partnerships between government, industry and the public to ensure that the UK is safer online. It will provide cyber incident response and be the UK's authoritative voice on cyber security. For the first time, key sectors will be able to engage directly with NCSC staff to get the best possible advice and support on securing networks and systems from cyber threats.

The NCSC provides:

- a unified source of advice for the Government's cyber security threat intelligence and information assurance;
- the strong public face of the Government's action against cyber threats – working hand in hand with industry, academia and international partners to keep the UK protected against cyber attack; and
- a public-facing organisation with reach back into GCHQ to draw on necessarily secret intelligence and world-class technical expertise.

There will be a phased approach to building the NCSC's capabilities over the lifetime of this strategy. It brings together the capabilities already developed by CESG – the information security arm of GCHQ – the Centre for the Protection of National Infrastructure (CPNI), CERT-UK (Computer Emergency Response Team) and the Centre for Cyber Assessment (CCA), enabling us to build on the best of what we already have, whilst greatly simplifying the former arrangements. Its initial focus will be:

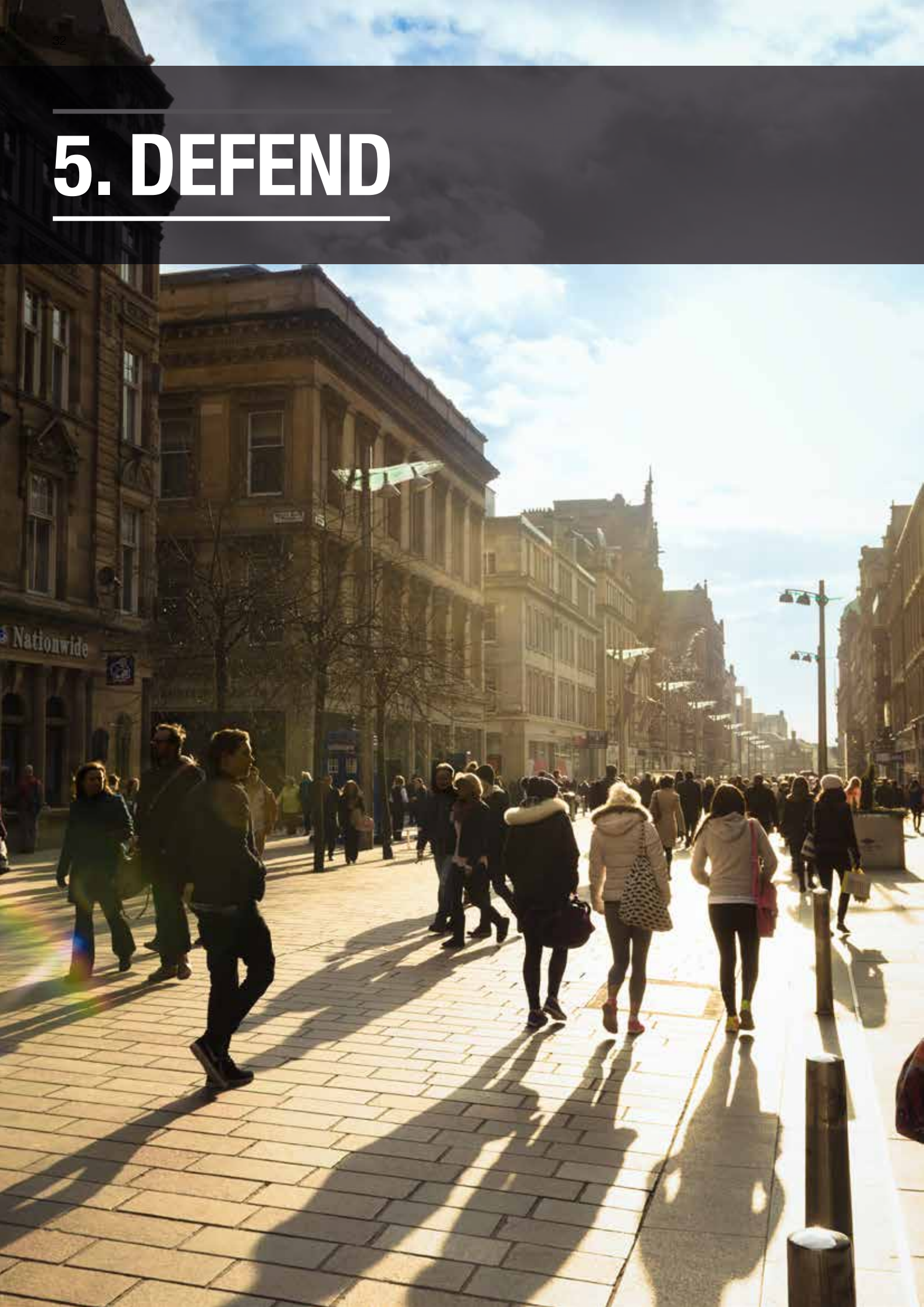
- a world class incident management capability to respond to and reduce the harm from cyber incidents – from those affecting single organisations through to national, large scale attacks;
- providing communications on how organisations in the public and private sector can deal with cyber security issues, facilitating the sharing of cyber threat information; and
- continuing to provide expert sectoral advice to Government and critical sectors like telecommunications, energy and finance, and providing cyber security advice across the UK.

The NCSC offers an effective means for the Government to deliver many elements of this strategy. We recognise that, as the NCSC grows, its focus and capabilities will need to adapt to new challenges and lessons learned.

IMPLEMENTATION PLAN

Our goals for the country's cyber security over the next five years are rightly ambitious. To achieve them will require us to act with consequence and determination across the digital landscape. Activity to deliver the Government's vision will advance the three primary objectives of the strategy: to DEFEND our cyberspace, to DETER our adversaries and to DEVELOP our capabilities, all underpinned by effective INTERNATIONAL ACTION.

5. DEFEND



5.0.1. The DEFEND elements of this strategy aim to ensure that UK networks, data and systems in the public, commercial and private spheres are resilient to and protected from cyber attack. It will never be possible to stop every cyber attack, just as it is not possible to stop every crime. However, together with citizens, education providers, academia, businesses and other governments, the UK can build layers of defence that will significantly reduce our exposure to cyber incidents, protect our most precious assets, and allow us all to operate successfully and prosperously in cyberspace. Acting to promote cooperation between states and good cyber security practice is also in the interest of our collective security.

5.0.2. The Government will implement measures to ensure that citizens, businesses, public and private sector organisations and institutions have access to the right information to defend themselves. The National Cyber Security Centre provides a unified source of advice in government for threat intelligence and information assurance, ensuring that we can offer tailored guidance for cyber defence and respond quickly and effectively to major incidents in cyberspace. The Government will work with industry and international partners to define what good cyber security looks like for public and private sectors, for our most important systems and services, and for the economy as a whole. We will build security by default into all new government and critical systems. Law enforcement agencies will collaborate closely with industry and the National Cyber Security Centre to provide dynamic criminal threat intelligence with which industry can better defend itself, and to promote protective security advice and standards.

5.1. ACTIVE CYBER DEFENCE

5.1.1. Active Cyber Defence (ACD) is the principle of implementing security measures to strengthen a network or system to make it more robust against attack. In a commercial context, Active Cyber Defence normally refers to cyber security analysts developing an understanding of the threats to their networks, and then devising and implementing measures to proactively combat, or defend, against those threats. In the context of this strategy, the Government has chosen to apply the same principle on a larger scale: the Government will use its unique expertise, capabilities and influence to bring about a step-change in national cyber security to respond to cyber threats. The 'network' we are attempting to defend is the entire UK cyberspace. The activities proposed represent a defensive action plan, drawing on the expertise of NCSC as the National Technical Authority to respond to cyber threats to the UK at a macro level.

Objectives

5.1.2. In undertaking ACD, the Government aims to:

- make the UK a much harder target for state sponsored actors and cyber criminals by increasing the resilience of UK networks;
- defeat the vast majority of high-volume/low-sophistication malware activity on UK networks by blocking malware communications between hackers and their victims;
- evolve and increase the scope and scale of Government's capabilities to disrupt serious state sponsored and cyber criminal threats;
- secure our internet and telecommunications traffic from hijacking by malicious actors;

- harden the UK's critical infrastructure and citizen-facing services against cyber threats; and
- disrupt the business model of attackers of every type, to demotivate them and to reduce the harm that their attacks can cause.

Approach

5.1.3. In pursuit of these aims, the Government will:

- work with industry, especially Communications Service Providers (CSPs), to make it significantly harder to attack UK internet services and users, and greatly reduce the prospect of attacks having a sustained impact on the UK. This will include tackling phishing, blocking malicious domains and IP addresses, and other steps to disrupt malware attacks. It will also include measures to secure the UK's telecommunications and internet routing infrastructure;
- increase the scale and development of GCHQ, Ministry of Defence and NCA capabilities to disrupt the most serious cyber threats to the UK, including campaigns by sophisticated cyber criminals and hostile foreign actors; and
- better protect government systems and networks, help industry build greater security into the CNI supply chain, make the software ecosystem in the UK more secure, and provide automated protections for government online services to the citizen.

5.1.4. Where possible, these initiatives will be delivered with or through partnerships with industry. For many, industry will be designing and leading implementation, with the Government's critical contribution being expert support, advice and thought-leadership.

5.1.5. The Government will also undertake specific actions to implement these measures, which will include:

- working with CSPs to block malware attacks. We will do this by restricting access to specific domains or web sites that are known sources of malware. This is known as Domain Name System (DNS) blocking / filtering;
- preventing phishing activity that relies on domain 'spoofing' (where an email appears to be from a specific sender, such as a bank or government department, but is actually fraudulent) by deploying an email verification system on government networks as standard and encouraging industry to do likewise;
- promoting security best practice through multi-stakeholder internet governance organisations such as the Internet Corporation for Assigned Names and Numbers (ICANN) which coordinates the domain name system), the Internet Engineering Task Force (IETF) and the European Regional Internet Registry (RIPE) and engagement with stakeholders in the UN Internet Governance Forum (IGF);
- working with law enforcement channels in order to protect UK citizens from being targeted in cyber attacks from unprotected infrastructure overseas;

- working towards the implementation of controls to secure the routing of internet traffic for government departments to ensure that it cannot be illegitimately re-routed by malicious actors; and
- investing in programmes in the Ministry of Defence, the NCA and GCHQ that will enhance the capabilities of these organisations to respond to, and disrupt, serious state-sponsored and criminal cyber activity targeting UK networks.

We will develop these technical interventions as threats evolve to ensure that UK citizens and businesses are protected by default from the majority of large-scale commodity cyber attacks.

Measuring success

5.1.6. The Government will measure its success in establishing effective ACD by assessing progress towards the following outcomes:

- the UK is harder to 'phish', because we have large-scale defences against the use of malicious domains, more active anti-phishing protection at scale and it is much harder to use other forms of communication, such as 'vishing' and SMS spoofing, to conduct social engineering attacks;
- a far larger proportion of malware communications and technical artefacts associated with cyber attacks and exploitation are being blocked;
- the UK's internet and telecommunications traffic is significantly less vulnerable to rerouting by malicious actors;
- GCHQ, the Armed Forces' and NCA capabilities to respond to serious state-sponsored and criminal threats have significantly increased.

5.2. BUILDING A MORE SECURE INTERNET

5.2.1. Changing technology provides us with the opportunity to significantly reduce the ability of our adversaries to conduct cyber crime in the UK by ensuring that future online products and services coming into use are 'secure by default'. That means ensuring that the security controls built into the software and hardware we use are activated as a default setting by the manufacturer so that the user experiences the maximum security offered to them, unless they actively choose to turn it off. The challenge is to effect transformative change in a way that supports the end user and offers a commercially viable, but secure, product or service – all within the context of maintaining the free and open nature of the Internet.

"Internet-connected things are multiplying rapidly. We saw many proof-of-concept and real world attacks in 2015, identifying serious vulnerabilities in cars, medical devices and more. Manufacturers need to prioritise security to reduce the risk of serious personal, economic and social consequences."

Symantec 2016 Internet Security Threat Report

5.2.2. The Government is well-placed to take a lead role in exploring those new technologies that will better protect our own systems, help industry build greater security into the supply chain, secure the software ecosystem and provide automated protections to citizens accessing government services online. The Government must test and implement new technologies that provide automated protection for government online products and services. Where possible, similar technologies should be offered to the private sector and the citizen.

Objective

5.2.3. The majority of online products and services coming into use become 'secure by default' by 2021. Consumers will be empowered to choose products and services that have built-in security as a default setting. Individuals can switch off these settings if they choose to do so but those consumers who wish to engage in cyberspace in the most secure way will be automatically protected.

Our approach

5.2.4. We will pursue the following actions:

- the Government will lead by example by running secure services on the Internet that do not rely on the Internet itself being secure;
- the Government will explore options for collaboration with industry to develop cutting-edge ways to make hardware and software more 'secure by default'; and
- we will adopt challenging new cyber security technologies in government, encouraging Devolved Administrations to do likewise, in order to reduce perceived risks of adoption. This will provide proof of concept and demonstrate the security benefits of new technologies and approaches. It will also put security at the heart of new product development, eliminate opportunities for criminal exploitation and thereby protect the end user.

5.2.5. To do this we will:

- continue to encourage hardware and software providers to sell products with security settings activated as default, requiring the user to actively disable these settings to make them insecure. Some vendors are already doing this, but some are not yet taking these necessary steps;
- continue to develop an Internet Protocol (IP) reputation service to protect government digital services (this would allow online services to get information about an IP address connecting to them, helping the service make more informed risk management decisions in real time);
- seek to install products on government networks that will provide assurance that software is running correctly, and not being maliciously interfered with;
- look to expand beyond the GOV.UK domain into other digital services measures that notify users who are running out-of-date browsers; and
- invest in technologies like Trusted Platform Modules (TPM) and emerging industry standards such as Fast Identity Online (FIDO), which do not rely on passwords for user authentication, but use the machine and other devices in the user's possession to authenticate. The Government will test innovative authentication mechanisms to demonstrate what they can offer, both in terms of security and overall user experience.

5.2.6. The Government will also explore how to encourage the market by providing security ratings for new products, so that consumers have clear information on

which products and services offer them the greatest security. The Government will also explore how to link these product ratings to new and existing regulators, and ways to warn consumers when they are about to take an action online that might compromise their security.

Measuring success

5.2.7. The Government will measure its success in building a secure Internet by assessing progress towards the following outcomes:

- the majority of commodity products and services available in the UK in 2021 are making the UK more secure because they have their default security settings enabled by default or have security integrated into their design; and
- all government services provided at national, local and Devolved Administration level are trusted by the UK public because they have been implemented as securely as possible, and fraud levels are within acceptable risk parameters.

5.3. PROTECTING GOVERNMENT

5.3.1. The UK Government, Devolved Administrations and the wider public sector hold large quantities of sensitive data. They deliver essential services to the public and operate networks that are critical to national security and resilience. The Government's systems underpin the functioning of our society. The modernisation of public sector services will continue to be the cornerstone of the UK's Digital Strategy – the Government's digital ambition is for the UK to be the world's leading digital nation. To retain the trust of citizens in online public sector services and systems, data held by government must be protected and all branches of government must implement appropriate levels of cyber security in the face of continuous attempts by hostile actors to gain access to government and public sector networks and data.

Objectives

5.3.2. We want to achieve the following outcomes:

- citizens use government online services with confidence: they trust that their sensitive information is safe and, in turn, understand their responsibility to submit their sensitive information online in a secure manner;
- the Government will set and adhere to the most appropriate cyber security standards, to ensure that all branches of government understand and meet their obligations to secure their networks, data and services; and
- the Government's critical assets, including those at the highest classification, are protected from cyber attacks.

Our approach

5.3.3. The UK Government will continue to move more of its services online so that the UK can become truly 'digital by default'. The Government Digital Service (GDS), the Crown Commercial Service (CCS) and the NCSC will ensure that all new digital services built or procured by government are also 'secure by default'.

5.3.4. The Government's networks are highly complex and in many cases still incorporate legacy systems, as well as some commercially available software which is no longer supported by the vendor. We will ensure that there are no unmanaged risks from legacy systems and unsupported software.

5.3.5. We will improve government and wider public sector resilience to cyber

attack. This means ensuring an accurate and up to date knowledge of all systems, data, and those who have access to them. The likelihood and impact of a cyber incident will be minimised by implementing best practice as set out by the NCSC. The Government will also ensure that it is able to respond effectively to cyber incidents through a programme of incident exercises and regular testing of government networks. We will invite Devolved Administrations and local authorities to participate in these exercises, as appropriate. Through automated scanning, we will ensure that we have a better knowledge of government's online security status.

5.3.6. Cyber security is not just about technology. Almost all successful cyber attacks have a contributing human factor. We will therefore continue to invest in our people, to ensure that everyone who works in government has a sound awareness of cyber risk. We will develop specific cyber expertise in areas where the risks are heightened and ensure that we have the right processes in place to manage these risks effectively.

5.3.7. The NCSC will develop world-leading cyber security guidance which will keep pace with the threat and development of new technologies. We will take steps to make sure government organisations have easy access to threat information to inform their understanding of their own cyber risks and take appropriate action.

5.3.8. We will continue to improve our highest classification networks to safeguard the Government's most sensitive communications.

5.3.9. Health and care systems pose unique challenges in the context of cyber security. The sector employs around 1.6 million people in over 40,000 organisations, each with vastly differing information security resources and capability. The National Data Guardian for Health and Care has set new data security standards for the health and social care systems in England, alongside a new data consent/opt-out model for patients. The Government will work with health and social care organisations to implement these standards.

"Britain is a world leader in cyber security, but with growing threats, this new Cyber Security Operations Centre will ensure our Armed forces continue to operate securely. Our increasing defence budget means that we can stay ahead of our adversaries in cyberspace while also investing in conventional capabilities"

The Rt Hon Michael Fallon MP,
Defence Secretary, April 2016

5.3.10. Cyber security is vital to our defence. Our Armed Forces depend on information and communications systems, both in the UK and on operations around the world. The infrastructure and personnel of the Ministry of Defence (MoD) are prominent targets. Defence systems are regularly targeted by criminals, foreign intelligence services and other malicious actors seeking to exploit personnel, disrupt business and operations, and corrupt and steal information. We will enhance cyber threat awareness, detection, and reaction functions, through the development of a Cyber Security Operations Centre (CSOC) that uses state-of-the-art defensive cyber capabilities to protect the MoD's cyberspace and deal with threats. The CSOC will work closely with the NCSC to confront the MoD's cyber security challenges and contribute to wider national cyber security.

Measuring success

5.3.11. The Government will measure its success in protecting government networks, systems and data by assessing progress towards the following outcomes:

- the Government has an in-depth understanding of the level of cyber security risk across the whole of government and the wider public sector;
- individual government departments and other bodies protect themselves in proportion to their level of risk and to an agreed government minimum standard;
- government departments and the wider public sector are resilient and can respond effectively to cyber incidents, maintaining functions and recovering quickly;
- new technologies and digital services deployed by government will be cyber secure by default;
- we are aware of, and actively mitigating, all known internet-facing vulnerabilities in government systems and services; and
- all suppliers to the Government meet appropriate cyber security standards.

5.4. PROTECTING OUR CRITICAL NATIONAL INFRASTRUCTURE AND OTHER PRIORITY SECTORS

Context

5.4.1 The cyber security of certain UK organisations is of particular importance because a successful cyber attack on them would have the severest impact on the country's national security. This impact could have a bearing on the lives of UK citizens, the stability and strength of the UK economy, or the UK's international standing and reputation. This premium group of companies and organisations within the public and private sector includes the critical national infrastructure

(CNI), which provides essential services to the nation. Ensuring the CNI is secure and resilient against cyber attack will be a priority for the Government. This premium group also includes other companies and organisations, beyond the CNI, that require a greater level of support. They include:

- the jewels in our economic crown – the UK's most successful companies and also those that hold our future economic strength in the value of their research and intellectual property;
- data holders – not just organisations that hold large amounts of personal data, but also those that hold data on vulnerable citizens here and abroad, such as charities;
- high-threat targets – such as media organisations, where an attack could harm the UK's reputation, damage public confidence in the Government, or endanger freedom of expression;
- the touchstones of our digital economy – digital service providers that enable e-commerce and our digital economy, and who depend on consumer trust in their services; and
- those organisations that, through market forces and authority, can exert influence on the whole economy to improve their cyber security, such as insurers, investors, regulators and professional advisors.

5.4.2. More needs to be done to protect these vital parts of our economy and support the organisations that heavily influence others. Our CNI – in both the private and public sector – continues to be a target for attack. Across these and many other priority sectors cyber risk is still not properly understood or managed, even as the threat continues to diversify and increase.

Objective

5.4.3. the UK Government, working with the Devolved Administrations and other responsible authorities where appropriate, will ensure that the UK's most important organisations and companies, including the CNI, are sufficiently secure and resilient in the face of cyber attack. Neither the Government nor other public bodies will take on the responsibility to manage this risk for the private sector, which rightly sits with boards, owners and operators. But the Government will provide support and assurance proportionate both to the threat these companies and organisations face, and to the consequences of their being attacked.

"Cyber security is key to unlocking innovation and expansion, and by adopting a tailored organisation and risk-centric approach to cyber security, organisations can refocus on opportunities and exploration. Building trust in a business that operates successfully within the Internet of Things (IoT), and that fully supports and protects individuals and their personal mobile devices (from a simple phone to a health care device, from smart appliances to smart cars), is a key competitive differentiator and must be a priority."

EY's Global Information Security Survey 2015

Our approach

5.4.4. Organisations and company boards are responsible for ensuring their networks are secure. They must identify critical systems and regularly assess their vulnerability against an evolving technological landscape and threat. They must invest in technology and their staff to reduce vulnerabilities in current and future systems, and in their supply chain, to maintain a level of cyber security proportionate to the risk. They must also have tested capabilities in place to respond if an attack happens. For the CNI, they must do this with government bodies and regulators so we can be confident that cyber risk is being properly managed and – if it is not – intervene in the interests of national security.

5.4.5. The Government will, therefore, understand the level of cyber security across our CNI and have measures in place to intervene where necessary to drive improvements that are in the national interest.

5.4.6. The Government will:

- share threat information with industry that only the Government can obtain so they know what they must protect themselves against;
- produce advice and guidance on how to manage cyber risk and, working collaboratively with industry and academia, define what good cyber security looks like;
- stimulate the introduction of the high-end security needed to protect the CNI, such as training facilities, testing labs, security standards and consultancy services; and
- conduct exercises with CNI companies to assist them in managing their cyber risks and vulnerabilities.

5.4.7. The NCSC will provide these services for the UK's most important companies and organisations, including the CNI. It will do so in partnership with departments and regulators, who will assure whether cyber risk is being managed in their sectors to the level demanded by the national interest.

5.4.8. The Government will also make sure that the right regulatory framework for cyber security is in place, one that:

- ensures industry acts to protect itself from the threat;
- is outcome focused and sufficiently flexible so that it will not fall behind the threat, or lead to compliance rather than sound risk management;
- is agile enough to foster growth and innovation, rather than lead it;
- is harmonised with regimes in other jurisdictions so that UK companies do not suffer from a fragmented and burdensome approach; and
- delivers, when combined with effective support from the Government, a competitive advantage for the UK.

5.4.9. Many of our industry sectors are already regulated for cyber security. Nonetheless, we must ensure the right steps are taken across the whole economy, including the CNI, to manage cyber security risks.

Measuring success

5.4.10. The Government will measure its success in protecting our CNI and other priority sectors by assessing progress towards the following outcomes:

- we understand the level of cyber security across the CNI, and have measures in place to intervene, where necessary, to drive improvements in the national interest; and

- our most important companies and organisations understand the level of threat and implement proportionate cyber security practices.

5.5. CHANGING PUBLIC AND BUSINESS BEHAVIOURS

5.5.1 A successful UK digital economy relies upon the confidence of businesses and the public in online services. The UK The Government has worked with industry and other parts of the public sector to increase awareness and understanding of the threat. The Government has also provided the public and business with access to some of the tools that they need to protect themselves. While there are many organisations that are doing an excellent job – in places, world-leading – of protecting themselves, and in providing services to others online, the majority of businesses and individuals are still not properly managing cyber risk.

"Last year, the average cost of breaches to large businesses that had them was £36,500. For small firms the average cost of breaches was £3,100. 65% of large organisations reported they had suffered an information security breach in the past year, and 25% of these experienced a breach at least once a month. Nearly seven out of ten attacks involved viruses, spyware or malware that might have been prevented using the Government's Cyber Essentials scheme."

2016 Government Cyber Health Check and Cyber Security Breaches Survey

Objective

5.5.2. Our objective is to ensure that individuals and organisations, regardless of size or sector, are taking appropriate steps to protect themselves, and their customers, from the harm caused by cyber attacks.

Our approach

5.5.3. The Government will provide the advice that the economy needs to protect itself. We will improve how this advice is delivered to maximise its effect. For the public, the Government will harness 'trusted voices' to increase the reach, credibility and relevance of our message. We will provide advice that is easy to act upon and relevant to individuals, at the point they are accessing services and exposing themselves to risk. We will involve the Devolved Administrations and other authorities as appropriate.

5.5.4. For businesses, we will work through organisations such as insurers, regulators and investors which can exert influence over companies to ensure they manage cyber risk. In doing so, we will highlight the clear business benefits and the pricing of cyber risk by market influencers. We will seek to understand better why many organisations still fail to protect themselves adequately and then work in partnership with organisations such as professional standards bodies, to move beyond raising awareness to persuade companies to take action. We will also make sure we have the right regulatory framework in place to manage those cyber risks the market fails to address. As part of this, we will seek to use levers, such as the GDPR, to drive up standards of cyber security and protect citizens.

5.5.5. Individuals and organisations and organisations in the UK will have access to the information, education, and tools they need to protect themselves. To ensure we deliver a step-change in public behaviour,

we will maintain a coherent and consistent set of messages on cyber security guidance from both the Government and our partners. The NCSC will provide technical advice to underpin this guidance. It will reflect business and public priorities and practices, and be clear, easily accessible and consistent, while keeping pace with the threat. Law enforcement will work closely with industry and the NCSC to share the latest criminal threat intelligence, to support industry to defend itself against threats, and to mitigate the impact of attacks on UK victims.

Measuring success

5.5.6. The Government will measure its success in protecting our CNI and other priority sectors by assessing progress towards the following outcomes:

- the UK economy's level of cyber security is as high as, or higher than, comparative advanced economies;
- the number, severity and impact of successful cyber attacks against businesses in the UK has reduced, because cyber hygiene standards have improved; and
- there is an improving cyber security culture across the UK because organisations and the public understand their cyber risk levels and understand the cyber hygiene steps they need to take to manage those risks.

CYBER AWARE

The Cyber Aware campaign, formerly Cyber Streetwise, gives the public the advice they need to protect themselves from cyber criminals. Targeted messaging delivered through social media and advertising and in partnership with businesses promotes:

- using three random words to create a strong password; and
- always downloading the latest software updates.

Experts agree adopting these behaviours will provide small businesses and individuals with protection against cyber crime. Cyber Aware is currently supported by 128 cross-sector partners, including the police and businesses in the retail, leisure, travel and professional services sectors. In 2015/16 an estimated 10 million adults and 1 million small businesses stated they were more likely to maintain or take up key cyber security behaviours as a result of the Cyber Aware campaign.

To find out more visit cyberaware.gov.uk

CYBER ESSENTIALS

The Cyber Essentials scheme was developed to show organisations how to protect themselves against low-level "commodity threat". It lists five technical controls (access control; boundary firewalls and Internet gateways; malware protection; patch management and secure configuration) that organisations should have in place. The vast majority of cyber attacks use relatively simple methods which exploit basic vulnerabilities in software and computer systems. There are tools and techniques openly available on the Internet which enable even low-skill actors to exploit these vulnerabilities. Properly implementing the Cyber Essentials scheme will protect against the vast majority of common internet threats.

5.6. MANAGING INCIDENTS AND UNDERSTANDING THE THREAT

5.6.1. The number and severity of cyber incidents affecting organisations across the public and private sector are likely to increase. We therefore need to define how both the private sector and the public engage with the Government during a cyber incident. We will ensure that the UK Government's level of support for each sector – taking into account its cyber maturity – is clearly defined and understood. The Government's collection and dissemination of information about the threat must be delivered in a manner and at a speed suitable for all types of organisation. The private sector, government and the public can currently access multiple sources of information, guidance and assistance on cyber security. This must be simplified.

5.6.2. We must ensure that the Government offering, both in response to incidents, and in the provision of guidance, does not exist in isolation, but in partnership with the private sector. Our incident management processes should reflect a holistic approach to incidents, whereby we learn from partners and share mitigation techniques. We will also continue to use our relationships with other Computer Emergency Response Teams (CERTs) and our allies as an integrated part of our incident management function.

5.6.3. Current incident management remains somewhat fragmented across government departments and this strategy will create a unified approach. The NCSC will deliver a streamlined and effective government-led incident response function. In the event of a serious cyber incident, we will ensure that the Armed Forces are able to provide assistance, whether in a conventional form addressing the physical impact of an incident, or in the form of specialist support from regular or reserve cyber personnel. While we will provide all the support our resources will allow, the Government continues to stress the importance of industry, society and the public acting to safeguard their basic cyber security.

Objectives

5.6.4. Our objectives are as follows:

- the Government will provide a single, joined-up approach to incident management, based on an improved understanding and awareness of the threat and actions being taken against us. The NCSC will be a key enabler, as will partnership with the private sector, law enforcement and other government departments, authorities and agencies;
- the NCSC defines clear processes for reporting incidents, tailored to the profile of the victim; and
- we will prevent the most common cyber incidents, and we will have effective information-sharing structures in place to inform 'pre-incident' planning.

Our approach

5.6.5. It is the responsibility of organisation and company management, in both the public and private sector, to ensure their networks are secure and to exercise incident response plans. In the event of a significant incident, the Government incident management process will reflect the three distinct elements of a cyber incident: the precursor causes, the incident itself and the post-incident response.

5.6.6. To deliver incident management that is effective for both government and the private sector, we will work closely to review and define the scope of the Government response to ensure it

reinforces cooperation. We will build on our national cyber exercise plan, using our improved understanding and awareness of the threat, to improve our offer of support to public and private sector partners.

5.6.7. We will create a trusted and credible government identity for incident advice, assistance and assurance. This will increase the cyber security awareness across the UK digital community and will enable us the better to identify trends, take pro-active measures and, ultimately, prevent incidents.

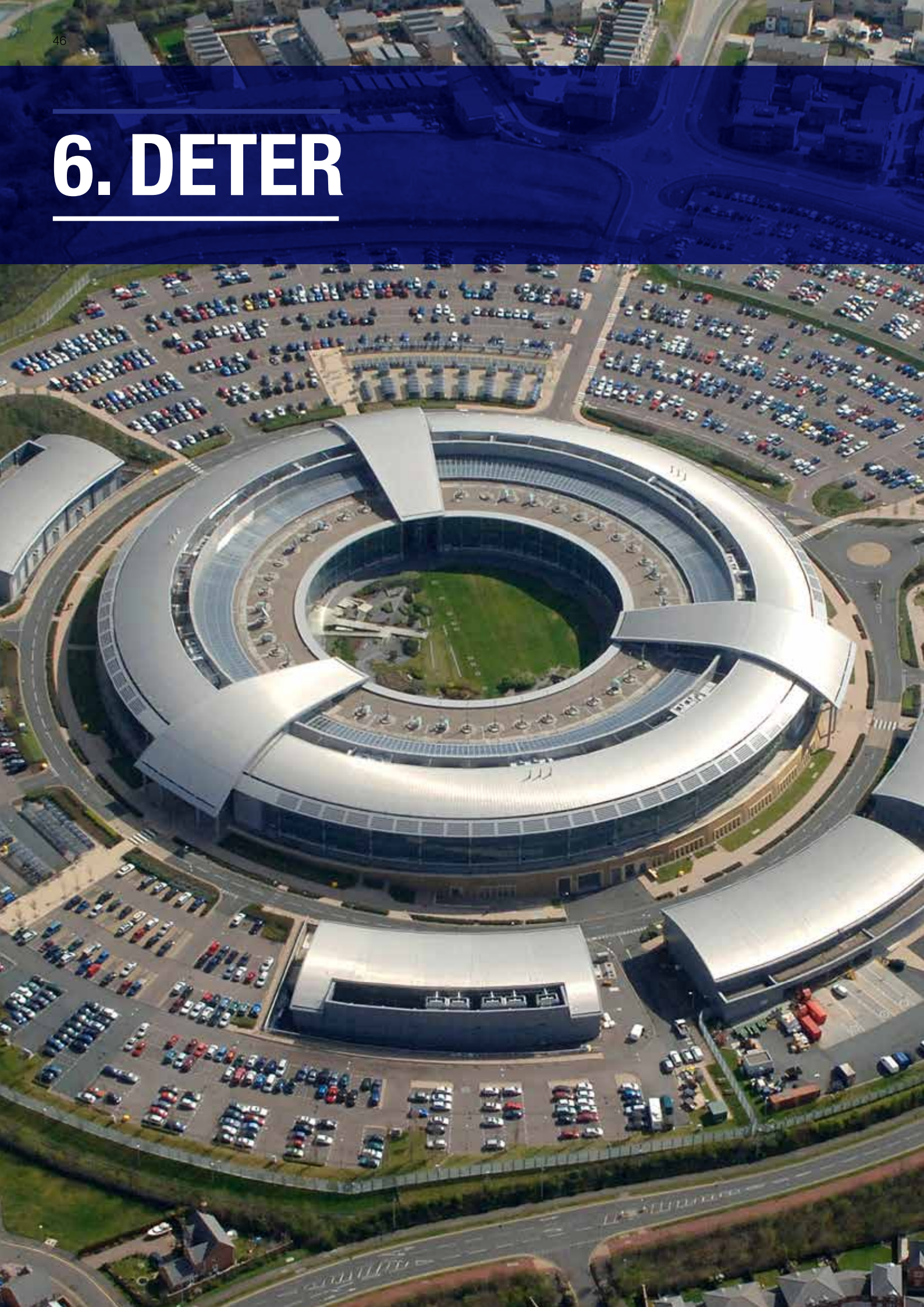
5.6.8. In moving towards automated information sharing (i.e. cyber security systems automatically alerting each other to incidents or attacks), we will deliver a more effective service. This will allow organisations to act swiftly on relevant threat information.

Measuring success

5.6.9. The Government will measure its success in managing incidents by assessing progress towards the following outcomes:

- a higher proportion of incidents are reported to the authorities, leading to a better understanding of the size and scale of the threat;
- cyber incidents are managed more effectively, efficiently and comprehensively, as a result of the creation of the NCSC as a centralised incident reporting and response mechanism; and
- we will address the root causes of attacks at a national level, reducing the occurrence of repeated exploitation across multiple victims and sectors.

6. DETER



6.0.1. The National Security Strategy states that defence and protection start with deterrence. This is as true in cyberspace as any other sphere. To realise our vision of a nation that is secure and resilient to cyber threats, and prosperous and confident in the digital world, we have to dissuade and deter those who would harm us and our interests. To achieve this we all need to continue to raise levels of cyber security so that attacking us in cyberspace – whether to steal from us or harm us – is neither cheap nor easy. Our adversaries must know that they cannot act with impunity: that we can and will identify them, and that we can act against them, using the most appropriate response from amongst all the tools at our disposal. We will continue to build global alliances and promote the application of international law in cyberspace. We will also more actively disrupt the activity of all those who threaten us in cyberspace and the infrastructure on which they rely. Delivering this ambition requires world-class sovereign capabilities.

6.1. CYBER'S ROLE IN DETERRENCE

6.1.1. Cyberspace is only one sphere in which we must defend our interests and sovereignty. Just as our actions in the physical sphere are relevant to our cyber security and deterrence, so our actions and posture in cyberspace must contribute to our wider national security.

6.1.2. The principles of deterrence are as applicable in cyberspace as they are in the physical sphere. The UK makes clear that the full spectrum of our capabilities will be used to deter adversaries and to deny them opportunities to attack us. However, we recognise that cyber security and resilience are in themselves a means of deterring attacks that rely on the exploitation of vulnerabilities.

6.1.3. We will pursue a comprehensive national approach to cyber security and deterrence that will make the UK a harder target, reducing the benefits and raising the costs to an adversary – be they political, diplomatic, economic or strategic. We must ensure our capability and intent to respond are understood by potential adversaries in order to influence their decision-making. We shall have the tools and capabilities we need: to deny our adversaries easy opportunities to compromise our networks and systems; to understand their intent and capabilities; to defeat commodity malware threats at scale; and to respond and protect the nation in cyberspace.

6.2. REDUCING CYBER CRIME

6.2.1. We need to raise the cost, raise the risk, and reduce the reward of cyber criminals' activity. While we must harden the UK against cyber attacks and reduce vulnerabilities, we must also focus relentlessly on pursuing criminals who continue to target the UK.

6.2.2. Law enforcement agencies will focus their efforts on pursuing the criminals who persist in attacking UK citizens and businesses. We will work with domestic and international partners to target criminals wherever they are located, and to dismantle their infrastructure and facilitation networks. Law enforcement agencies will also continue to help raise awareness and standards of cyber security, in collaboration with the NCSC.

6.2.3. This strategy complements the 2013 Serious and Organised Crime Strategy, which set out the UK Government's strategic response to cyber crime, alongside other types of serious and organised crime. The National Cyber Crime Unit (NCCU) that sits within the National Crime Agency (NCA) was established to lead and coordinate the national response to cyber crime. Action Fraud provides a national reporting centre for fraud and cyber crime. A network of cyber crime units within Regional Organised Crime Units (ROCUs) provide access to specialist cyber capabilities at a regional level, supporting the NCCU and local forces.

Objective

6.2.4. We will reduce the impact of cyber crime on the UK and its interests by deterring cyber criminals from targeting the UK and relentlessly pursuing those who persist in attacking us.

Our approach

6.2.5. To reduce the impact of cyber crime, we will:

- enhance the UK's law enforcement capabilities and skills at national, regional and local level to identify, pursue, prosecute and deter cyber criminals within the UK and overseas;
- build a better understanding of the cyber crime business model, so we know where to target interventions in order to have the most disruptive effect on criminal activity. We will use this knowledge to:
  - make the UK a high-cost, high-risk environment in which to operate by targeting the UK nexus of criminality, and by working with industry to reduce the ability of criminals to exploit UK infrastructure; and
  - tackle cyber crime upstream, adding friction to the criminal business model by dismantling their infrastructure and financial networks, and wherever possible, bringing offenders to justice.
- build international partnerships to end the perceived impunity of cyber criminals acting against the UK, by bringing criminals in overseas jurisdictions to justice;
- deter individuals from being attracted to, or becoming involved in, cyber crime by building on our early intervention measures;
- enhance collaborations with industry to provide them with proactive intelligence on the threat, and to provide us with the upstream intelligence that they possess, in order to assist with our upstream disruption efforts;
- develop a new 24/7 reporting and triage capability in Action Fraud, linked to the NCSC, the NCA's National Cyber Crime Unit and the wider law enforcement community, to improve support to victims of cyber crime, to provide a faster response to reported crimes and enhanced protective security advice. A new reporting system will be established to share information in real time across law enforcement on cyber crime and threats;
- work with the NCSC and the private sector to reduce vulnerabilities in UK infrastructure that could be exploited at scale by cyber criminals; and
- work with the finance sector to make the UK a more hostile environment for those seeking to monetise stolen credentials, including by disrupting their networks.

Measuring success

6.2.6. The Government will measure its success in reducing cyber crime by assessing progress towards the following outcomes:

- we have a greater disruptive effect on cyber criminals attacking the UK, with higher numbers of arrests and convictions, and larger numbers of criminal networks dismantled as a result of law enforcement intervention;
- there is improved law enforcement capability, including greater capacity and skills of dedicated specialists and mainstream officers and enhanced law enforcement capability amongst overseas partners;
- there is improved effectiveness and increased scale of early intervention measures dissuades and reforms offenders; and
- there are fewer low-level cyber offences as a result of cyber criminal services being harder to access and less effective.

WHAT TO DO IF YOU ARE A VICTIM OF CYBER CRIME

If you are a member of the public and you believe that you are the victim of cyber crime, or cyber enabled fraud, you should contact Action Fraud.

You can report the incident using Action Fraud's online fraud reporting tool anytime of the day or night, or call 0300 123 2040. For further information see www.actionfraud.police.uk

The Action Fraud service is run by the City of London Police.

6.3. COUNTERING HOSTILE FOREIGN ACTORS

6.3.1. We need to bring to bear the full range of government capabilities to counter the threat posed by hostile foreign actors that increasingly threaten our political, economic and military security. Working with international partners will be key to our success, and greater emphasis will be placed on engaging them and working with them to counter the threat. Much of this action will not be in the public domain. Our investment in sovereign capabilities and partnerships with industry and the private sector will continue to underpin our ability to detect, observe and identify this constantly evolving activity against us.

Objective

6.3.2. We will have strategies, policies and priorities in place for each adversary, to ensure a proactive, well-calibrated and effective approach is taken to counter the threat and in order to drive down the number and severity of cyber incidents in the future.

Our approach

6.3.3. To reduce the cyber threat from hostile foreign actors, we will:

- reinforce the application of international law in cyberspace in addition to promoting the agreement of voluntary, non-binding norms of responsible state behaviour and the development and implementation of confidence building measures;
- work with international partners, particularly through collective defence, cooperative security, and enhanced deterrence that our membership of NATO affords;
- identify both the unique and generic aspects of our adversaries' cyber activity;

- generate and explore all available options for deterring and countering this threat, drawing on the full range of government capabilities. We will take full account of other related factors, including country-specific strategies, international cyber priorities, and cyber crime and prosperity objectives;
- use existing networks and relationships with our key international partners to share information about current and nascent threats, adding value to existing thought and expertise; and
- attribute specific cyber identities publicly when we judge it in the national interest to do so.

Measuring success

6.3.4. The Government will measure its success in countering the actions of hostile foreign actors by assessing progress towards the following outcomes:

- the stronger information-sharing networks that we have established with our international partners, and wider multilateral agreements in support of lawful and responsible behaviour by states, are substantially contributing to our ability to understand and respond to the threat, resulting in a better defended UK; and
- our defence and deterrence measures, alongside our country-specific strategies, are making the UK a harder target for hostile foreign actors to act against.

6.4. PREVENTING TERRORISM

6.4.1. The technical capability of terrorists currently remains limited but they continue to aspire to conduct damaging computer network operations against the UK, with publicity and disruption as the primary objective of their cyber activity. The Government will identify and disrupt terrorists using and intending to use cyber for this purpose. In doing so, we will minimise their impact and prevent an uplift in terrorist cyber capability that would further threaten UK networks and national security.

Objective

6.4.2. To mitigate the threat of terrorist use of cyber, through the identification and disruption of terrorist cyber actors who currently hold, and aspire to build, capability that could threaten UK national security.

Our approach

6.4.3. To ensure the threat posed by cyber terrorism remains low, we will:

- detect cyber terrorism threats, identifying actors who are seeking to conduct damaging network operations against the UK and our allies;
- investigate and disrupt these cyber terrorism actors to prevent them from using cyber capability against the UK and its allies; and
- work closely with international partners to enable us to better tackle the threat from cyber terrorism.

Measuring success

6.4.4. The Government will measure its success in preventing terrorism by assessing progress towards the following outcomes:

- a full understanding of risk posed by cyber terrorism, through identification and investigation of cyber terrorism threats to the UK; and
- close monitoring, and disruption of terrorist cyber capability at the earliest opportunity, with the aim of preventing an increase in such terrorist capability in the long term.

6.5. ENHANCING SOVEREIGN CAPABILITIES – OFFENSIVE CYBER

6.5.1. Offensive cyber capabilities involve deliberate intrusions into opponents' systems or networks, with the intention of causing damage, disruption or destruction. Offensive cyber forms part of the full spectrum of capabilities we will develop to deter adversaries and to deny them opportunities to attack us, in both cyberspace and the physical sphere. Through our National Offensive Cyber Programme (NOCP), we have a dedicated capability to act in cyberspace and we will commit the resources to develop and improve this capability.

Objective

6.5.2. We will ensure that we have at our disposal appropriate offensive cyber capabilities that can be deployed at a time and place of our choosing, for both deterrence and operational purposes, in accordance with national and international law.

Our approach

6.5.3. To do this, we will:

- invest in our NOCP – the partnership between the Ministry of Defence and GCHQ that is harnessing the skills and talents of both organisations to deliver the tools, techniques and tradecraft required;
- develop our ability to use offensive cyber tools; and
- develop the ability of our Armed Forces to deploy offensive cyber capabilities as an integrated part of operations, thereby enhancing the overall impact we can achieve through military action.

Measuring success

6.5.4. The Government will measure our success in establishing offensive cyber capabilities by assessing progress towards the following outcomes:

- the UK is a world leader in offensive cyber capability; and
- the UK has established a pipeline of skills and expertise to develop and deploy our sovereign offensive cyber capabilities.

6.6. ENHANCING SOVEREIGN CAPABILITIES – CRYPTOGRAPHY

6.6.1. Cryptographic capability is fundamental to protecting our most sensitive information and to choosing how we deploy our Armed Forces and national security capabilities. To maintain this capability, we will require private sector skills and technologies that are assured by GCHQ. This is likely to require work to be done in the UK, by British Nationals with the requisite security clearance, working for companies who are prepared to be completely open with GCHQ in discussing design and implementation details. The MOD and GCHQ are working to establish a sound understanding of the long-term cost implications of maintaining such sovereign cryptographic capabilities, based on prevailing market conditions and in cooperation with those companies currently able to provide such solutions.

Objective

6.6.2. We have the confidence that the UK will always have political control over those cryptographic capabilities vital to our national security and, therefore, the means to protect UK secrets.

Our approach

6.6.3. We will select the means that allow us to share information effectively with our allies, and ensure that trusted information and information systems are available, when and where required. Working closely with other government departments and agencies, GCHQ and MOD will together define sovereign requirements, and how best to meet those requirements when suppliers must be domestic. This will be delivered through a new joint framework for determining requirements for operational advantage and freedom of action.

Measuring success

6.6.4. The Government will measure its success in maintaining our cryptographic capabilities by assessing progress towards the following outcome:

- our sovereign cryptographic capabilities are effective in keeping our secrets and sensitive information safe from unauthorised disclosure.

ENCRYPTION

Encryption is the process of encoding data or information to prevent unauthorised access to it.

The Government is in favour of encryption. It is a foundation stone of a strong, internet-based economy: it keeps people's personal data and intellectual property secure, and ensures safe online commerce.

But as technology continues to evolve, we have to ensure that there are no guaranteed 'safe spaces' for terrorists and criminals to operate beyond the reach of the law.

The Government wants to work with industry as technology develops to ensure that, with a robust legal framework and clear oversight, the police and intelligence agencies can access the content of the communications of terrorists and criminals. Existing legislation allows for the communications of criminals and terrorists to be intercepted when a warrant is in place. Companies have a duty to give effect to such a warrant, providing the requested communications, to the relevant authority. When served with a warrant, companies are asked to remove any encryption that they themselves have applied, or that has been applied on their behalf, so that the material provided is in readable form. The law stipulates that companies are required to take reasonable steps to give effect to a warrant, and any assessment of reasonableness will include an assessment of the steps a company is required to take to remove encryption.

7. DEVELOP

7.0.1. The DEVELOP strand of the strategy sets out how we will acquire and strengthen the tools and capabilities that the UK needs to protect itself from the cyber threat.

7.0.2. The UK requires more talented and qualified cyber security professionals. The Government will act now to plug the growing gap between demand and supply for key cyber security roles, and inject renewed vigour into this area of education and training. This is a long-term, transformative objective, and this strategy will kick-start this important work, which will necessarily continue beyond 2021. A skilled workforce is the lifeblood of a vital and world leading cyber security commercial ecosystem. This ecosystem will ensure cyber start-ups prosper and receive the investment and support they need. This innovation and vigour can only be provided by the private sector; but the Government will act to support its development, and actively promote the wider cyber security sector to the world market. A dynamic and thriving scientific research sector is required to support both the development of highly skilled people, and to ensure that new ideas translate into cutting-edge products.

7.1. STRENGTHENING CYBER SECURITY SKILLS

7.1.1. The UK needs to tackle the systemic issues at the heart of the cyber skills shortage: the lack of young people entering the profession; the shortage of current cyber security specialists; insufficient exposure to cyber and information security concepts in computing courses; a shortage of suitably qualified teachers; and the absence of established career and training pathways into the profession.

7.1.2. This calls for swift intervention by the Government to help address the current shortage and develop a coherent long-term strategy that can build on these interventions to close the skills gap. However, it must be recognised that to have any profound impact, this effort must be collaborative, with input from a range of participants and influencers across the Devolved Administrations, public sector, education providers, academia bodies and industry.

Objective

7.1.3. The Government's ambition is to ensure the sustained supply of the best possible home-grown cyber security talent, whilst funding specific interventions in the short term to help meet known skills gaps. We will also define and develop the cyber security skills needed across the population and workforce to operate safely and securely online.

7.1.4. This requires action over the next twenty years, not just the next five. We will define the long-term, coordinated set of actions needed by government, industry, education providers and academia to establish a sustained supply of competent cyber security professionals, who meet the requisite standards and certification to practise confidently and securely.

7.1.5. We will close the skills gap in Defence. We will attract cyber specialists to government who are not only effectively trained but also ready to maintain our national security. This includes an understanding of the impact of cyberspace on military operations.

Our approach

7.1.6. We will develop and implement a self-standing skills strategy that builds on existing work to integrate cyber security into the education system. This will continue to improve the state of computer science teaching overall and embed cyber

security into the curriculum. Everyone studying computer science, technology or digital skills will learn the fundamentals of cyber security and will be able to bring those skills into the workforce. As part of this effort, we will address the gender imbalance in cyber-focused professions, and reach people from more diverse backgrounds, to make sure we are drawing from the widest available talent pool. We will work closely with the Devolved Administrations to encourage a consistent approach across the UK.

7.1.7. We will set out more clearly the respective roles of government and industry, including how these might evolve over time. The UK Government and Devolved Administrations have a key role in creating the right environment for cyber security skills to be developed and to update the education system to reflect the changing needs of industry and government. But employers also have a significant responsibility to clearly articulate their needs, as well as train and develop employees and young people entering the profession. Industry has an important role in building diverse and attractive career and training pathways in partnership with academia, professional bodies and trade associations.

7.1.8. In recognition of the collective challenge we face in closing the skills gap, we will establish a skills advisory group formed of government, employers, professional bodies, skills bodies, education providers and academia, which will strengthen the coherence between these key sectors. This group will support the development of a long-term strategy which will take account of developments in the broad field of digital skills, ensuring that cyber security considerations are aligned and incorporated throughout. This group will work with similar bodies across the UK.

7.1.9. Alongside this work, the Government will invest in a range of initiatives to bring about immediate improvements and inform the development of the long-term skills strategy. These include:

- establishing a schools programme to create a step change in specialist cyber security education and training for talented 14-18 year olds (involving classroom-based activities, after-school sessions with expert mentors, challenging projects and summer schools);
- creating higher and degree-level apprenticeships within the energy, finance and transport sectors to address skills gaps in essential areas;
- establishing a fund to retrain candidates already in the workforce who show a high potential for the cyber security profession;
- identifying and supporting quality cyber graduate and post graduate education, and identifying and filling any specialist skills gaps – acknowledging the key role that universities play in skills development;
- supporting the accreditation of teacher professional development in cyber security. This work will help teachers, and others supporting learning, to understand cyber security education and provide a method of externally accrediting such individuals;
- developing the cyber security profession, including through achieving Royal Chartered status by 2020, reinforcing the recognised body of cyber security excellence within the industry and providing a focal point which can advise, shape and inform national policy;
- developing a Defence Cyber Academy as a centre of excellence for cyber training and exercise across the Ministry of Defence and wider Government, addressing specialist skills and wider education;

- developing opportunities for collaboration in training and education between government, the Armed Forces, industry and academia, together with facilities to maintain and exercise skills; and
- we will work with industry to expand the CyberFirst programme to identify and nurture the diverse young talent pool to defend our national security; and
- embedding cyber security and digital skills as an integral an integral part of relevant courses within the education system, from primary to postgraduate levels, setting standards, improving quality and providing a firm foundation for onwards progression into the field.

As education is a devolved matter, some of these initiatives will apply mainly in England. We will however work with the Devolved Administrations to encourage a consistent approach across the UK education systems.

Measuring success

7.1.10. The Government will measure our success in strengthening cyber security skills by assessing progress towards the following outcomes:

- there are effective and clear entry routes into the cyber-security profession, which are attractive to a diverse range of people;
- by 2021 cyber security is taught effectively as an integral part of relevant courses from primary to post-graduate level;
- cyber security is widely acknowledged as an established profession with clear career pathways, and has achieved Royal Chartered Status;
- appropriate cyber security knowledge is an integral part of the continual professional development for relevant non-cyber security professionals, across the economy; and
- the Government and the Armed Forces and the Armed Forces have access to cyber specialists able to maintain the security and resilience of the UK.

7.2. STIMULATING GROWTH IN THE CYBER SECURITY SECTOR

7.2.1. A burgeoning and innovative cyber security sector is a necessity for our modern, digital economy. UK cyber security firms provide world-leading technologies, training and advice to industry and governments. But whilst the UK is a leading player, it faces fierce competition to stay ahead. There are also barriers that the Government needs to address. UK companies and academics develop cutting-edge technology, but some require support to develop the commercial and entrepreneurial skills required to thrive. There are funding gaps that prevent SMEs from growing and expanding into new markets and territories. The most ground-breaking products and services, that offer the potential to keep us ahead of the threat, struggle to find customers who are willing to act as early adopters. Overcoming these challenges requires government, industry and academia to work effectively together.

Objective

7.2.2. The Government will support the creation of a growing, innovative and thriving cyber security sector in the UK in order to create an ecosystem where:

- security companies prosper, and get the investment they need to grow;
- the best minds from government, academia and the private sector collaborate closely to spur innovation; and
- customers of the Government and industry are sufficiently confident and prepared to adopt cutting-edge services.

Our approach

7.2.3. To create this ecosystem, we will:

- commercialise innovation in academia, providing training and mentoring to academics;
- establish two innovation centres, to drive the development of cutting-edge cyber products and dynamic new cyber security companies, which will sit at the heart of a programme of initiatives to give start-ups the support they need to get their first customers and attract further investment;
- allocate a proportion of the £165m Defence and Cyber Innovation Fund to support innovative procurement in defence and security;
- provide testing facilities for companies to develop their products, together with a fast-track form of assessment for the next generation of cyber security products and services as they emerge, enabling customers to be confident in their use;
- draw on the collective expertise of the industry-government Cyber Growth Partnership to help shape and focus further growth and innovation interventions;
- help companies of all sizes scale-up and access international markets; and
- promote agreed international standards that support access to the UK market.

7.2.4. We will also use the weight of government procurement to spur innovation. The Government faces some of the hardest challenges in cyber security, and some of the biggest threats. We can, and must, pursue the most effective solutions to these problems. That means making it easier for smaller companies to do business with government. It also means the Government must be less risk averse in testing and using new products. This is a win-win solution: the Government will get the best services, and innovative technology will get an early adopter, making it easier to attract investment and a larger customer base. We will encourage all parts of government, including the Devolved Administrations, to take a similar approach.

> "We want to create a cyber ecosystem in which cyber start-ups proliferate, get the investment and support they need to win business around the world, to provide a pipeline of innovation that channels ideas between the private sector, government and academia."
>
> The Rt Hon Matt Hancock MP, Minister of State for Digital and Culture

Measuring success

7.2.5. The Government will measure its success in stimulating growth in the cyber security sector by assessing progress towards the following outcomes:

- greater than average global growth in the size of the UK cyber sector year on year;
- a significant increase in investment in early stage companies;
- adoption of more innovative and effective cyber security technologies in government.

7.3. PROMOTING CYBER SECURITY SCIENCE AND TECHNOLOGY

7.3.1. The UK's thriving science and technology sector and its cutting-edge research, underpins our world-leading cyber security capabilities. To maintain and enhance the UK's reputation as a global leader in cutting-edge research, we need our academic research establishments to continue to attract the best and the brightest minds in the field of cyber security. This will require us to foster centres of excellence that attract the most able and dynamic scientists and researchers, and deepen the active partnership between academia, the Government and industry. This will involve a match-making role for the Government, where we incentivise such collaborations. Success would see us establish a self-sustaining ecosystem that allows ideas – and people – to circulate between the three sectors in a mutually beneficial way.

Objective

7.3.2. By 2021, the UK will have strengthened its position as a world leader in cyber science and technology. Flexible partnerships between universities and industry will translate research into commercially successful products and services. The UK will maintain its reputation for innovative excellence, including in those areas of exceptional national strength, such as the financial sector.

Our approach

7.3.3. To achieve this, the Government will encourage collaboration, innovative and flexible funding models for research, and the commercialisation of research. Government will ensure that the human and behavioural aspects of cyber are given sufficient attention, and that systems beyond the technical, such as business processes and organisational structures, are included within cyber science and technology.

7.3.4. This will underpin the creation of products, systems and services that are 'secure by default', with appropriate security considered from the outset and where security becomes a conscious 'opt-out' for users.

7.3.5. We will publish a detailed Cyber Science and Technology Strategy after a thorough consultation with partners and stakeholders. This will include identifying areas of science and technology that the Government, industry and academia consider to be important and identifying gaps in the UK's current capacity to address them.

7.3.6. The Government will continue to provide funding and support for the Academic Centres of Excellence, Research Institutes and Centres for Doctoral Training. In addition, we will create a new Research Institute in a strategically important subject area. We will also fund further research in those areas where the upcoming Cyber Science and Technology Strategy identifies capability gaps. Important areas that will be given consideration include: big data analytics; autonomous systems; trustworthy

industrial control systems; cyber-physical systems and the Internet of Things; smart cities; automated system verification; and the science of cyber security.

7.3.7. We will continue to sponsor UK national PhD students at the Academic Centres of Excellence to increase the number of UK nationals with cyber expertise.

7.3.8. The Government will work with bodies, including Innovate UK and the Research Councils to encourage collaboration between industry, the Government and academia. To support this collaboration we will review best practice concerning security classifications and identify security-cleared experts, including academics. This will ensure that work from the unclassified space to beyond secret can be as collaborative as possible.

7.3.9. The Government will fund a 'grand challenge' to identify and provide innovative solutions to some of the most pressing problems in cyber security. CyberInvest, a new industry and Government partnership to support cutting-edge cyber security research and protect the UK in cyberspace, will be part of our approach to building the academic-government-industry partnership.

Measuring success

7.3.10. The Government will measure its success in promoting cyber security science and technology by assessing progress towards the following outcomes:

- significantly increased numbers of UK companies successfully commercialising academic cyber research and fewer agreed and identified gaps in the UK's cyber security research capability with effective action to close them; and
- the UK is regarded as a global leader in cyber security research and innovation.

7.4. EFFECTIVE HORIZON SCANNING

7.4.1. The Government must ensure that policy-making takes account of the changing cyber, geopolitical and technology landscape. To do this, we need to make effective use of broad horizon scanning and assessment work. We need to invest in proofing ourselves against future threats and anticipate market changes that might affect our cyber resilience in five to ten years' time. We need horizon scanning programmes that generate recommendations to inform current and future government policy and programme planning.

Objective

7.4.2. The Government will ensure that our horizon scanning programmes include a rigorous assessment of cyber risk, and that this is integrated into cyber security and other technology policy development areas, along with all-source assessment and other available evidence. We will join up horizon scanning between national security and other policy areas to ensure a holistic assessment of emerging challenges and opportunities.

Our approach

7.4.3. We will:

- identify gaps in current work, and coordinate work across disciplinary boundaries to develop a holistic approach to horizon scanning for cyber security;
- promote better integration of technical aspects of cyber security with behavioural science;
- support rigorous monitoring of the cyber criminal market place to spot new tools and services that might enable technology transfer to hostile states, terrorists or criminals;

- analyse emergent internet-connected process control technologies;
- anticipate vulnerabilities around digital currencies; and
- monitor market trends in telecommunications technologies to develop early defences against anticipated future attacks.

7.4.4. We recognise that horizon scanning goes beyond the technical, to include political, economic, legislative, social and environmental dimensions. Cyber security is just one aspect of the issues that effective horizon scanning can help to address. Therefore, we will ensure that where we conduct horizon scanning of these other policy areas, we will take into account any cyber security implications.

7.4.5. We will also ensure that cyber policy-making follows an evidence-based approach, taking into account assessments from all available sources. This will include, for example:

- specific technical evidence, for example on the Internet of Things, or the future role of advanced materials; and
- international strategic and societal trends and their impact on cyber.

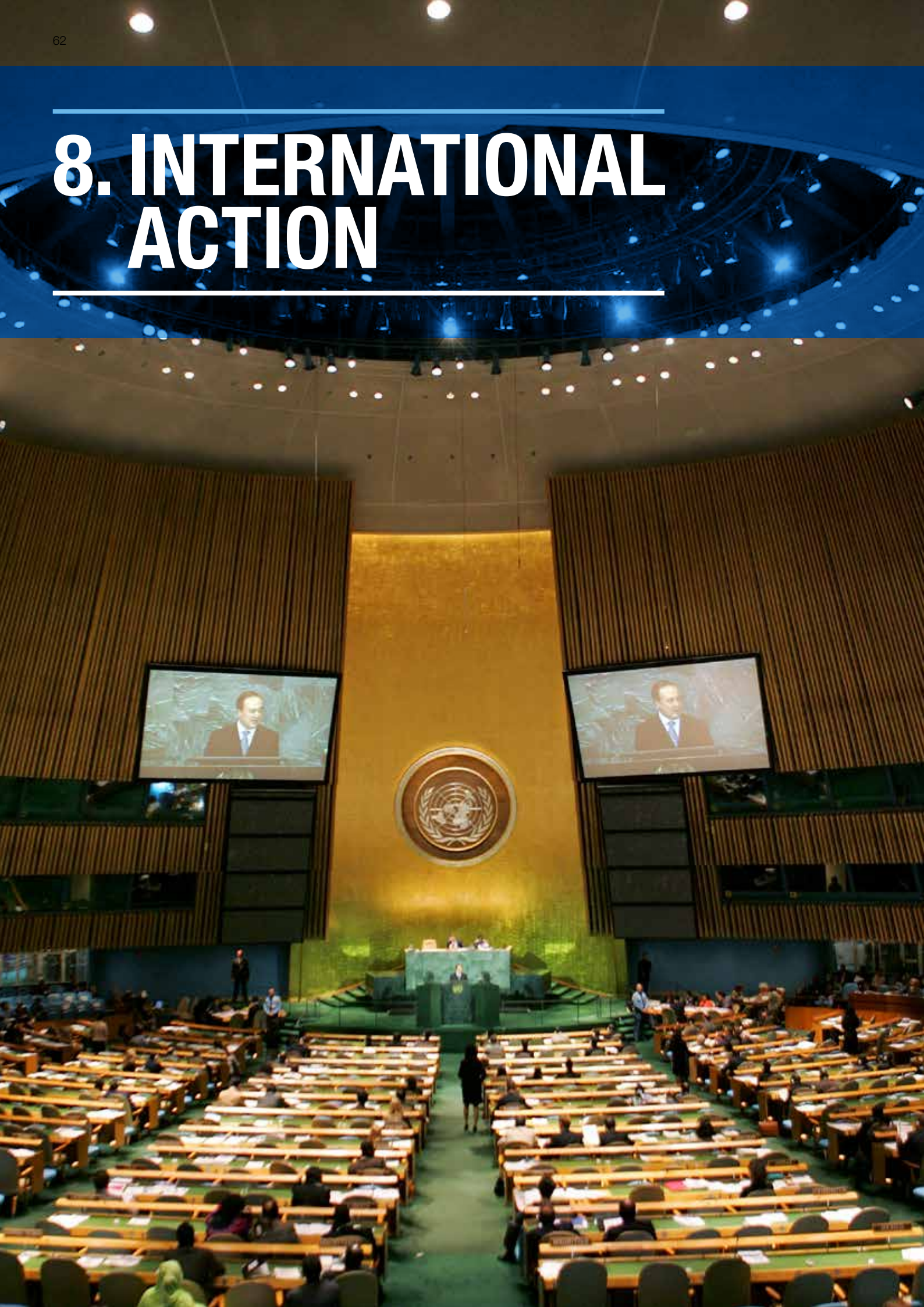
7.4.6. We will ensure that cyber security is considered within the remit of the cross-Government Emerging Technology and Innovation Analysis Cell (ETIAC), which will be established to identify technology threats and opportunities relevant to national security and that cyber is considered by existing horizon-scanning structures, including the Government Futures Group (GFG), and the Cabinet Secretary's Advisory Group on horizon scanning (CSAG).

Measuring success

7.4.7. The Government will measure our success in establishing an effective horizon scanning capability by assessing progress towards the following outcomes:

- cross-government horizon scanning and all-source assessment are integrated into cyber policy making; and
- the impact of cyber security is factored into all cross-government horizon scanning.

8. INTERNATIONAL ACTION



8.1. Our economic prosperity and social wellbeing increasingly depend on the openness and security of networks that extend beyond our own borders. It is essential that we work closely with international partners to ensure the continuation of a free, open, peaceful and secure cyberspace that delivers these benefits. This will only become more important as the next billion users come online across the globe.

8.2. International cooperation on cyber issues has become an essential part of wider global economic and security debates. It is a rapidly evolving area of policy, without a single agreed international vision. The UK and its allies have been successful in ensuring some elements of the rules-based international system are in place: there has been agreement that international law applies in cyberspace; that human rights apply online as they do offline; and a broad consensus that the multi-stakeholder approach is the best way to manage the complexities of governing the Internet. However, with a growing divide over how to address the common challenge of reconciling national security with individual rights and freedoms, any global consensus remains fragile.

"We must work internationally to agree the rules of the road that will ensure the UK's future security and prosperity in cyberspace."

The Rt. Hon. Boris Johnson, MP, Foreign Secretary

Objectives

8.3. The UK aims to safeguard the long-term future of a free, open, peaceful and secure cyberspace, driving economic growth and underpinning the UK's national security. On this basis, the UK will continue to: champion the multi-stakeholder model of internet governance; oppose data localisation; and work to build the capacity of our partners to improve their own cyber security. In order to reduce the threat to the UK and our interests, much of which originates overseas, we will seek to influence the decision-making of those engaging in cyber crime, cyber espionage, and disruptive or destructive cyber activity and continue to build frameworks to support international cooperation.

Our Approach

8.4. To do this we will:

- strengthen and embed a common understanding of responsible state behaviour in cyberspace;
- build on agreement that international law applies in cyberspace;
- continue to promote the agreement of voluntary, non-binding, norms of responsible state behaviour;
- support the development and implementation of confidence-building measures;
- increase our ability to disrupt and prosecute cyber criminals based abroad, especially in hard-to-reach jurisdictions;
- help foster an environment which allows our law enforcement agencies to work together to ensure fewer places exist where cyber criminals can act without fear of investigation and prosecution;
- promote the resilience of cyberspace by shaping the technical standards governing emerging technologies

internationally (including encryption), making cyberspace more 'secure by design' and promoting best practice;
- work to build common approaches amongst like-minded countries for capabilities such as strong encryption, which have cross-border implications;
- build the capacity of others to tackle threats to the UK, and our interests overseas;
- continue to help our partners develop their own cyber security – since we share a single cyberspace, we collectively become stronger when each country improves its own defences;
- ensure that NATO is prepared for the conflicts of the 21st century, which will play out in cyberspace as well as on the battlefield;
- work with our allies to enable NATO to operate as effectively in cyberspace as it does on land, air and sea; and
- ensure that the 'London Process' of Global Conferences on Cyberspace continues to promote global consensus towards a free, open, peaceful and secure cyberspace.

8.5. There are a range of relationships and tools we will continue to invest in to deliver and underpin all our international cyber objectives; we cannot achieve our objectives in isolation. These include:

- working in concert with traditional allies and new partners to establish and maintain strong active political and operational relationships; creating the political conditions to build strong global alliances;
- using our influence with multilateral organisations such as the United Nations, G20, European Union, NATO, OSCE, Council of Europe, the Commonwealth and within the global development community; and
- building stronger relationships with non-government actors – industry, civil society, academia and the technical community. These actors are crucial in informing and challenging international policy formulation, and strengthening political messages on a wide range of cyber issues. Our world-class academic links provide a neutral, collaborative platform with international partners.

Measuring Success

8.6 The Government will measure its success in advancing our international interests in cyber by assessing progress towards the following outcomes:

- enhanced international collaboration reduces cyber threat to the UK and our interest overseas;
- a common understanding of responsible state behaviour in cyberspace;
- international partners have increased their cyber security capability; and
- strengthened international consensus on the benefits of a free, open, peaceful and secure cyberspace.

9. METRICS

9.1. Cyber security remains an area of relative immaturity when it comes to the measurement of outcomes and impacts – normally referred to as metrics. Already the science of cyber security has been obscured by hyperbole and obstructed by an absence of calibrated data. This is a source of frustration for policy-makers and businesses alike, who have struggled to measure investment against outcomes. The Government assesses that the effective use of metrics is essential for delivering this strategy and focussing the resources that underpin it.

9.2. We will ensure that this strategy is founded upon a rigorous and comprehensive set of metrics against which we measure progress towards the outcomes we need to achieve. As well as being a major deliverable under the Strategy in its own right, the NCSC will play a crucial role in enabling other parts of Government, industry and society to deliver all of these strategic outcomes within this strategy.

9.3. Annex 3 sets out how the success measures set out in the strategy will contribute to the strategic outcomes, which will be reviewed annually to ensure they accurately reflect our national goals and requirements. The headline, strategic outcomes are as follows:

1. The UK has the capability effectively to detect investigate and counter the threat from the cyber activities of our adversaries.

2. The impact of cybercrime on the UK and its interests is significantly reduced and cyber criminals are deterred from targeting the UK.

3. The UK has the capability to manage and respond effectively to cyber incidents to reduce the harm they cause to the UK and counter cyber adversaries.

4. Our partnerships with industry on active cyber defence mean that large scale phishing and malware attacks are no longer effective.

5. The UK is more secure as a result of technology products and services having cyber security designed into them and activated by default.

6. Government networks and services will be as secure as possible from the moment of their first implementation. The public will be able to use government digital services with confidence and trust that their information is safe.

7. All organisations in the UK, large and small, are effectively managing their cyber risk and are supported by high quality advice designed by the NCSC, underpinned by the right mix of regulation and incentives.

8. There is the right ecosystem in the UK to develop and sustain a cyber security sector that can meet our national security demands.

9. The UK has a sustainable supply of home grown cyber skilled professionals to meet the growing demands of an increasingly digital economy, in both the public and private sectors, and defence.

10. The UK is universally acknowledged as a global leader in cyber security research and development, underpinned by high levels of expertise in UK industry and academia.

11. The UK government is already planning and preparing for policy implementation in advance of future technologies and threats and is 'future proofed'.

12. The threat to the UK and our interests overseas is reduced due to increased international consensus and capability towards responsible state behaviour in a free, open, peaceful and secure cyberspace.

13. UK Government policies, organisations and structures are simplified to maximise the coherence and effectiveness of the UK's response to the cyber threat.

9.4. We recognise that some of our ambitions for this strategy go beyond its five year timescale. In order that any future investment in cyber beyond 2021 can continue to deliver the maximum transformative effect, we intend that these longer term outcomes are allocated beyond 2021 to industry, regulators, auditors, insurers and other parts of the public and private sector, as the effective management of cyber security risks is integrated into standard management activity for all.

CONCLUSION: CYBER SECURITY BEYOND 2021

10.1. The rapid evolution of the cyber landscape will constantly throw up new challenges as technology evolves and our adversaries act to exploit it. However, this strategy aims to provide a range of policies, tools and capabilities that will ensure we can respond quickly and flexibly to each new challenge as it arises.

10.2. Should we fail to act effectively, the threat will continue to outpace our ability to protect ourselves against it. We can expect an explosion of threat capability at all levels.

10.3. Conversely, if we realise these ambitions, all parts of UK government, business and society will play their part in delivering the country's overall cyber security. If we can ensure security is designed and built in, by default, into commodity technologies, consumers and businesses would have less cause to worry about cyber security. Should the UK consolidate its reputation as a secure environment to do business online, more global companies and investors will choose to locate here. Security for CNI networks and priority sectors would be more effective. Potential attackers looking to develop tools and attack methods against systems holding key functions and data would in turn have to work harder to overcome the layered security that surrounds them. This would change the risk versus reward equation for cyber criminals and malicious actors, who would expect to face the same threat of prosecution internationally as they do for traditional crimes. If we can succeed in mainstreaming cyber security across all parts of our society, it could mean that Government itself can step back from such a prominent role, allowing the market and the technology to drive the evolution of cyber security across the economy and society.

10.4. Even in the most optimistic scenario, some of the challenges the UK faces in the cyber domain, whether in scale or complexity, may need more than five years to address. This strategy nonetheless provides us with the means to transform our future security and safeguard our prosperity in the digital era.

ANNEXES

ANNEX 1: ACRONYMS

CCA – the Centre for Cyber Assessment. Based in the NCSC, it provides cyber threat assessments for UK government departments to inform policy.

CERT – Computer Emergency Response Team.

CERT-UK – National Computer Emergency Response Team in the UK.

CESG – the National Technical Authority for Information Assurance within the UK. It provides a trusted, expert, independent, research and intelligence-based service on information security on behalf of UK the government.

CNI – 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.

CPNI – the Centre for the Protection of National Infrastructure. It delivers advice that aims to reduce the vulnerability of organisations in the national infrastructure to terrorism and espionage. It will also work in partnership with NCSC to provide holistic protective security advice on threats from cyberspace. CPNI has built up strong partnerships with private sector organisations across the national infrastructure, creating a trusted environment where information can be shared for mutual benefit. Direct relationships are augmented by an extended network, which includes other government departments and professional service organisations.

DDoS – Distributed Denial of Service attack. The flooding of an information system with more requests than it can handle, resulting in authorised users being unable to access it.

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

ICT – Information and Communications Technology.

MOD – Ministry of Defence

NATO – North Atlantic Treaty Organisation.

NCA – National Crime Agency; a non-Ministerial government department.

NCSC – the National Cyber Security Centre.

OSCE – Organisation for Security and Cooperation in Europe.

SME – Small and medium-sized enterprises.

ANNEX 2: GLOSSARY

Action Fraud – the UK's national fraud and internet crime reporting centre, providing a central point of contact for the public and businesses.

Active Cyber Defence (ACD) – the principle of implementing security measures to strengthen the security of a network or system to make it more robust against attack.

Anonymisation – the use of cryptographic anonymity tools to hide or mask one's identity on the Internet.

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

Automated system verification – measures to ensure that software and hardware are working as expected, and without errors.

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

Big data – data sets which are too big to process and manage with commodity software tools in a timely way, and require bespoke processing capabilities to manage their volumes, speed of delivery and multiplicity of sources.

Bitcoin – a digital currency and payment system.

Commodity malware – malware that is widely available for purchase, or free download, which is not customised and is used by a wide range of different threat actors.

Computer Network Exploitation (CNE) – cyber espionage; the use of a computer network to infiltrate a target computer network and gather intelligence.

Cyber Crime marketplace – the totality of products and services that support the cyber crime ecosystem.

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

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 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.

CyberInvest – a £6.5m industry and government scheme to support cutting-edge cyber security research and protect the UK in cyberspace.

Cyber-physical system – systems with integrated computational and physical components; 'smart' systems.

Cyber resilience – the overall ability of systems and organisations to withstand cyber events and, where harm is caused, recover from them.

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 Challenge – competitions encouraging people to test their skills and to consider a career in cyber.

Cyberspace – the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, internet-connected devices and embedded processors and controllers. It may also refer to the virtual world or domain as an experienced phenomenon, or abstract concept.

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.

Domain Name System (DNS) – a naming system for computers and network services based on a hierarchy of domains.

Doxing – the practice of researching, or hacking, an individual's personally identifiable information on the Internet, then publishing it.

e-commerce – electronic commerce. Trade conducted, or facilitated by, the Internet.

Encryption – cryptographic transformation of data (called 'plaintext') into a form (called 'cipher text') that conceals the data's original meaning, to prevent it from being known or used.

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.

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.

Annex 2
GLOSSARY

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.

Industrial Internet of Things (IIoT) – the use of Internet of Things technologies in manufacturing and industry.

Insider – someone who has trusted access to the data and information systems of an organisation and poses an intentional, accidental or unconscious cyber threat.

Integrity – the property 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.

London Process – measures resulting from the 2011 London Conference on Cyberspace.

Malware – malicious software, or code. Malware includes viruses, worms, Trojans and spyware.

Network (computer) – a collection of host computers, together with the sub-network or inter-network, through which they can exchange data.

Offensive cyber – the use of cyber capabilities to disrupt, deny, degrade or destroy computers networks and internet-connected devices.

Patching – patching is the process of updating software to fix bugs and vulnerabilities

Penetration testing – activities designed to test the resilience of a network or facility against hacking, which are authorised or sponsored by the organisation being tested.

Phishing – the use of emails that appear to originate from a trusted source, to deceive recipients into clicking on malicious links or attachments that are weaponised with malware, or share sensitive information, with an unknown third party.

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

Reconnaissance – the phase of an attack where an attacker gathers information on, and maps networks, as well as probing them for exploitable vulnerabilities in order to hack them.

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

Router – devices that interconnect logical networks by forwarding information to other networks based upon IP addresses.

Script kiddie – a less skilled individual who uses ready-made scripts, or programs, that can be found on the Internet to conduct cyber attacks, such as web defacements.

Secure by default – the unlocking of the secure use of commodity technologies whereby security comes by default for users.

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

SMS spoofing – a technique which masks the origin of an SMS text message by replacing the originating mobile number (Sender ID) with alphanumeric text. It may be used legitimately by a sender to replace their mobile number with their own name, or company name, for instance. Or it may be used illegitimately, for example, to fraudulently impersonate another person.

Social engineering – the methods attackers use to deceive and manipulate victims into performing an action or divulging confidential information. Typically, such actions include opening a malicious webpage, or running an unwanted file attachment.

Trusted Platform Module (TPM) – an international standard for a secure cryptoprocessor, which is a dedicated microprocessor designed to secure hardware by integrating cryptographic keys into devices.

User – a person, organisation entity, or automated process, that accesses a system, whether authorised to, or not.

Virus – viruses are malicious computer programs that can spread to other files.

Vishing – vishing or 'voice phishing' is the use of voice technology (landline phones, mobile phones, voice email, etc) to trick individuals into revealing sensitive financial or personal information to unauthorised entities, usually to facilitate fraud.

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

ANNEX 3: HEADLINE IMPLEMENTATION PROGRAMME

NATIONAL CYBER SECURITY STRATEGY 2016-2021

Vision: the UK is secure and resilient to cyber threats; prosperous and confident in the digital world

Strategic outcomes	Indicative success measures (to 2021)	Contributes to
1. The UK has the capability to effectively detect, investigate and counter the threat from the cyber activities of our adversaries.	• The stronger information sharing networks that we have established with our international partners, and wider multilateral agreements in support of lawful and responsible behaviour by states, are substantially contributing to our ability to understand and respond to the threat, resulting in a better defended UK. • Our defence and deterrence measures, alongside our country-specific strategies, are making the UK a harder target for hostile foreign actors and cyber terrorists to succeed against. • Improved understanding of the cyber threat from hostile foreign and terrorist actors, through identification and investigation of cyber terrorism threats to the UK. • Ensuring that terrorist cyber capability remains low in the long term, through close monitoring of capability, and disruption of terrorist cyber potential and activity at the earliest opportunity. • The UK is a world leader in offensive cyber capability. • The UK has established a pipeline of skills and expertise to develop and deploy our sovereign offensive cyber capabilities. • Our sovereign cryptographic capabilities are effective in keeping our secrets and sensitive information safe from unauthorised disclosure.	DETER
2. The impact of cybercrime on the UK and its interests is significantly reduced and cyber criminals are deterred from targeting the UK.	• We are having a greater disruptive effect on cyber criminals attacking the UK, with increased numbers of arrests and convictions, and larger numbers of criminal networks dismantled as a result of law enforcement intervention. • Improved law enforcement capability, including: capacity and skills for both dedicated specialists and mainstream officers; and enhanced overseas law enforcement capability. • Improved effectiveness, and increased scale, of early intervention (“PREVENT”) measures is dissuading and reforming offenders. • A reduction in low-level cyber offences as a result of cyber criminal services being harder to access and less effective.	DETER
3. The UK has the capability to manage and respond effectively to cyber incidents to reduce the harm they cause to the UK and counter cyber adversaries.	• A higher proportion of incidents are reported to the authorities, leading to a better understanding of the size and scale of the threat. • Cyber incidents are managed more effectively, efficiently and comprehensively, as a result of the creation of the National Cyber Security Centre as a centralised incident reporting and response mechanism. • We will address the root causes of attacks at a national level, reducing the occurrence of repeated exploitation across multiple victims and sectors.	DEFEND

Strategic outcomes	Indicative success measures (to 2021)	Contributes to
4. Our partnerships with industry on active cyber defence mean that large scale phishing and malware attacks are no longer effective.	• The UK is harder to "phish", because we have large-scale defences against the use of malicious domains, more active anti-phishing protection at scale and it is much harder to use other forms of communication, such as 'vishing' and SMS spoofing, to conduct social engineering attacks. • A far larger proportion of malware communications and technical artefacts associated with cyber attacks and exploitation are being blocked. • The UK's internet and telecommunications traffic is significantly less vulnerable to rerouting by malicious actors. • GCHQ, Defence and NCA capabilities to respond to serious state-sponsored and criminal threats have significantly increased.	DEFEND
5. The UK is more secure as a result of technology products and services having cyber security designed into them and activated by default.	• The majority of commodity products and services available in the UK in 2021 are making the UK more secure, because they have their default security settings enabled by default or have security integrated into their design. • Government services are trusted by the UK public, because they have been implemented as securely as possible, and fraud levels against them are within acceptable risk parameters.	DEFEND
6. Government networks and services will be as secure as possible from the moment of their first implementation. The public will be able to use government digital services with confidence, and trust that their information is safe.	• Government has an in-depth understanding of the level of cyber security risk across the whole of government and the wider public sector. • Individual government departments and other bodies protect themselves in proportion to their level of risk and to an agreed government minimum standard. • Government departments and the wider public sector are resilient and can respond effectively to cyber incidents, maintaining functions and recovering quickly. • New technologies and digital services deployed by government will be cyber secure by default. • We are aware of, and actively mitigating, all known internet-facing vulnerabilities in government systems and services; • All government suppliers meet appropriate cyber security standards.	DEFEND

Annex 3
HEADLINE IMPLEMENTATION PROGRAMME

Strategic outcomes	Indicative success measures (to 2021)	Contributes to
7. All organisations in the UK, large and small, are effectively managing their cyber risk, are supported by high quality advice designed by the NCSC, underpinned by the right mix of regulation and incentives.	• We understand the level of cyber security across the CNI, and have measures in place to intervene, where necessary, to drive improvements in the national interest. • Our most important companies and organisations understand the level of threat and implement proportionate cyber security practices. • The UK economy's level of cyber security is as high as, or higher than, comparative advanced economies. • The number, severity and impact of successful cyber attacks against businesses in the UK has reduced, because cyber hygiene standards have been applied. • The UK has an improving cyber security culture, because organisations and the public understand their cyber risk levels, and understand the cyber hygiene steps they need to take to manage those risks.	DEFEND
8. There is the right ecosystem in the UK to develop and sustain a cyber security sector that can meet our national security demands.	• Greater than average global growth in the size of the UK cyber sector year on year. • A significant increase in investment in early stage companies.	DEVELOP
9. The UK has a sustainable supply of home grown cyber skilled professionals to meet the growing demands of an increasingly digital economy, in both the public and private sectors, and defence.	• There are effective and clear entry routes into the cyber-security profession, which are attractive to a diverse range of people. • By 2021 cyber security is taught effectively as an integral part of relevant courses within the education system, from primary to post-graduate level. • Cyber security is widely acknowledged as an established profession with clear career pathways, and has achieved Royal Chartered Status. • Appropriate cyber security knowledge is an integral part of the continual professional development for relevant non-cyber security professionals, across the economy. • Government and the armed forces have access to cyber specialists able to maintain the security and resilience of the UK.	DEVELOP

Strategic outcomes	Indicative success measures (to 2021)	Contributes to
10. The UK is universally acknowledged as a global leader in cyber security research and development, underpinned by high levels of expertise in UK industry and academia.	• The number of UK companies successfully commercialising academic cyber research has increased significantly. There are fewer agreed and identified gaps in the UK's cyber security research capability, and effective action has been taken to close them. • The UK is regarded as a global leader in cyber security research and innovation.	DEVELOP
11. The UK government is already planning and preparing for policy implementation in advance of future technologies and threats and is 'future proofed'.	• Cross-government horizon scanning work and all-source assessment are integrated into cyber policy making. • The impact of cyber security is factored into all cross-government horizon scanning work.	DEVELOP
12. The threat to the UK and our interests overseas is reduced due to increased international consensus and capability towards responsible state behaviour in a free, open peaceful and secure cyberspace.	• Enhanced international collaboration reduces cyber threat to the UK and our interest overseas; • A common understanding of responsible state behaviour in cyberspace; • International partners increased their cyber security capability; and • Strengthened international consensus on the benefits of a free, open, peaceful and secure cyberspace.	INTERNATION-AL ACTION AND INFLUENCE
13. UK Government policies, organisations and structures are simplified to maximise the coherence and effectiveness of the UK's response to the cyber threat.	• The Government cyber security responsibilities are understood and its services are accessible. • Our partners understand how best to interact with Government on cyber security issues	CROSS-CUTTING