**UK cybersecurity policy and implications for the 4th industrial revolution**

Hangjae Lee

The University of York,

MPA Comparative Applied Social and Public Policy, Evaluation and Research

2018.9.18 – 2020.7.17

**요 약**

**1. 추진배경**

4차 산업혁명을 위한 노력들이 선진국들은 물론 여러 개발도상국에서도 진행되고 있는 현실이다. 데이터, 네트워트, 인공지능의 발달을 위해 정부와 민간이 협업을 통해 노력하고 있다. 그러나, 최근 사이버 해킹 및 개인정보보호 유출 등 ICT 상에서의 범죄가 속출하고 있는 현실이다. 이에 따라 미국, 영국, 등 주요 선진국들은 국가 차원의 사이버 보안(Cyber security) 전략을 수립하였으며, 범부처 차원으로 정책을 추진하고 있다. 특히, 영국의 경우 금융 산업이 매우 발달하였기 때문에 사이버 해킹의 위협이 끊이지 않고 있는 나라이다. 그러다 보니, 영국의 사이버 보안 기술과 대응능력, 그리고 사이버 보안 기업들이 발전하였으며, 또한 정부 차원의 사이버 보안 정책을 지속적으로 발전시켜 오고 있다. 본 보고서에서는 영국의 최근 Cyber security 전략을 면밀히 분석하고 시사점을 도출해 보고자 한다.

동 보고서는 크게 3개의 파트로 구성되어 있다. 첫번째 파트는 정보보호와 사이버 보안의 개념 등 기본적인 개요를 설명한다. 두번째 파트는 영국의 ICT 현황에 대한 설명이다. 영국의 사이버보안을 책임지는 National cyber security center에 대한 설명과 ICT 발전 및 서비스 현황을 설명한다. 그리고 영국의 사이버 보안 발전 정도에 대해서도 분석을 한다. 세번째 파트는 영국의 사이버 보안전략에 대한 자세한 분석이다. 영국이 사이버 보안전략을 본격적으로 추진하는 주된 배경과 사이버 위협으로부터 국가와 기업 및 국민을 보호하기 위한 방안들이 소개된다. 그리고 사이버 보안 사업을 육성하기 위한 구체적인 전략이 마지막 부분에 자세하게 언급된다.

**2. 정보보안과 사이버 보안 개요**

1. **정보보안(Information security)**

정보보안의 정의는 출처에 따라 다양하다. 주요한 예시들은 아래와 같다.

* "정보의 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability). 추가적으로 진정성(authenticity), 책임성(accountability), 부인방지(non-repudiation), 그리고 신뢰성(reliability)과 관계가 있을 수 있다." (ISO/IEC 27000:2009)
* "인가되지 않은 접근, 사용, 폭로, 붕괴, 수정, 파괴로부터 정보와 정보 시스템을 보호해 기밀성, 무결성, 가용성을 제공하는 것." (CNSS, 2010)
* "인가된 사용자만이(기밀성) 정확하고 완전한 정보로(무결성) 필요할 때 접근할 수 있도록(가용성) 하는 일련의 작업." (ISACA, 2008)
* "조직의 지적 자산을 보호하는 절차." (Pipkin, 2000)
* "...정보보안은 위험 관리 규율로, 정보 위험이 사업에 미치는 비용을 관리하는 작업이다." (McDermott and Geer, 2001)
1. **사이버 보안 (Cyber security)**

사이버보안(Cybersecurity)은 컴퓨터와 네트워크, 데이터를 악의적인 전자적 공격으로부터 보호하는 전반적인 활동이다. 실제 세상에서 건물이나 다른 사물에 대한 액세스를 제어하는 보다 전통적인 보안 활동인 물리적 보안과 비교가 되는 활동이다. 첨단 기술에 바탕을 둔 물리적 보안업체도 많고, 조직도에 물리적 보안과 사이버보안이 결합되어 있는 경우도 있지만, 사이버보안은 사유지 침입이나 절도가 아닌 악의적 로그인과 코드로부터 자산을 보호하는 것에 초점이 맞춰진 활동이다.

3. **영국의 ICT 현황**

영국의 전반적인 ICT 발전 수준은 전 세계 5% 이내의 최상위권



출처: KISA, 2019

영국의 ICT 이용 및 보급률은 세계 최고 수준으로 우리나라와 비슷함



 출처: KISA, 2019

ITU의 글로벌 사이버 보안지수에서 영국 12위

* 2017년 11월 ITU의 사이버보안지수 자료에 의하면 영국은 전 세계에서 12위 순위로 한국(13위)보다 한 순위 앞서고, 유럽지역에서는 에스토니아, 프랑스, 노르웨이에 이어 4번째 순위에 해당함
* 특히 최근 들어 사이버 공간을 통한 각종 침투 공격과 테러 예방을 위해 국가 정보보호정책을 계속 강화하고 있는 추세로 관련 기기 및 솔루션,소프트웨어 등의 수요가 계속 증가해 나갈 것으로 전망

**4. 영국의 사이버보안 전략**

1. **사이버보안 전략 수립 배경**

2018년 1월 영국 국가사이버보안센터(National Cyber Security Centre)에서는 사이버 공격에 대해 총체적으로 완벽한 방어가 불가능함을 인정하고, 피해의 최소화를 강조함

2018년 10월 영국 국가사이버보안센터는 연례 보고서에서 러시아와 중국, 북한 등 적대적인 국가의 지시나 후원을 받거나, 이들 국가가 용인한 해커들에 의한 것이라고 발표하고, 사이버 공격을 위한 도구와 서비스 비용이 감소함에 따라 사이버 공격이 늘어날 것이라고 발표함(https://www.ncsc.gov.uk/news/annual-review-2018).

1. **국가 사이버보안 전략 계획**

영국은 정보보호 전략을 기본으로 세부 과제를 지속적으로 평가ᆞ관리하기 위해 매년 전략 추진과정 검토와 목표별 진행 현황을 발표하고 있다. 2016년 영국은 사이버 보안 전략 추진과정 검토와 함께 향후 전략 추진 방향을 담고 있는 ‘국가 사이버보안 전략 계획(National Cyber Security Strategy Our Forward Plans)’을 발표하였으며, 영국 사이버보안 전략의 4 가지 주요 목표를 중심으로 국가 대응능력 향상, 영국 주요기반 시설 및 네트워크 복원력 강화, 사이버인식 및 위험관리 능력 향상, 일반 국민의 사이버보안 인 식 제고 및 전문인력 양성, 국제협력 등에 관한 계획을 수립하고 있다

**< 목표 1: 사이버범죄 억제 및 안전한 사이버 공간 구현 >**

영국 정부는 사이버범죄 억제 및 안전한 사이버 공간 구현 목표를 달성하기 위해 사이버보안 위협에 관한 인식제고 및 효과적인 사이버보안 위험관리체계 확립을 목표로 민간 부문과의 협력을 강화하겠다는 계획을 밝혔다. 이를 위해 사이버보안정보 공유협력체(CISP)를 500 개까지 확대, 기업들을 위한 사이버보안 관련 지침서 제공, 업계 주도의 사이버보안 관련 표준화를 지원하는 등 안전한 사이버 공간 구현을 위해 민ᆞ관 협력을 주요한 내용으로 하고 있다. 특히, 고객이 시장에 접근하고 사업을 수행하는 것을 돕기 위해 사이버보안 전문가, 사이버보안 제품 및 서비스의 산업규격합격품표시(kite marking)를 확대하는 등 사이버보안 산업 육성에도 관심을 기울이고 있는 것으로 나타나 영국 산업 내 정보보호 인증제품 확산을 위한 노력도 추진되고 있다.

**< 목표 2: 사이버 공격에 대한 복원력 강화와 사이버 상의 권익 보호 >**

사이버 공격에 대한 복원력 강화와 사이버 상의 권익 보호의 목표를 위해 정부부처, 기관 등 자체 위험 관리제도 마련을 통한 사이버 위험 관리를 지원하고 주요 기반 시설 사업자들과의 사이버위협 정보 공유를 확대할 계획을 밝히고 있다. 그리고 이를 위해 네 트워크 복원력 강화와 같은 표준화된 접근방식을 포함하고 있는 공공부문 네트워크(Public Sector Network)를 구축하고, 모든 정부부처ᆞ정부기관 이사회의 자체 리스크 관리제도 를 통해 사이버 리스크 관리를 지원하는 등 사이버위협으로 부터의 복원력 강화를 위한 계 획을 밝히고 있다. 또한, 영국 컴퓨터비상대응팀(CERT-UK) 설립을 위한 관련 업계와의 파트너십 체결, 주요기반시설 사업자들과의 사이버 위협 정보 공유를 위한 사이버보안정 보공유협력체(CISP) 기능 확대를 추진하고자 하였다.

**< 목표 3: 열린, 역동적, 안정적인 사이버 공간 구현 >**

열린, 역동적, 안정적인 사이버 공간 구현의 목표를 달성하기 위해 사이버 공간에 대한 행동규범을 마련하고, 사이버 공간 내 기술과 정책을 선도할 수 있도록 국가 간, 기관 간 협력을 강화하겠다고 밝히고 있다. 이는 최근 사이버 공간 내 국경이 없는 만큼 국제적인 협력의 중요성이 강조됨에 따라 EU, NATO, 인도, 한국 등 국제기구와 국가 간의 협력을 확대하고, 공동 작업을 통한 영국의 사이버 공간의 가치를 전파하는데 노력을 기울이겠다 는 의미로 이해할 수 있다.

또한, 사이버 범죄 퇴치와 사이버 공간 내에서의 국제법 적용과 관련한 작업에서도 영 국의 입장을 반영할 수 있도록 국제회의에 적극 참여하여 국제 사이버보안 정책, 전략을 선도하겠다는 계획을 밝히고 있다.

**< 목표 4: 사이버보안 지식, 기술, 능력 구축 >**

영국은 사이버보안 지식, 기술, 능력 구축의 목표를 달성하기 위해 교육, 학계 및 산업 부문간 협력을 통한 사이버 인재를 양성하는 등 사이버보안 전문 인력의 수급을 강화하고 사이버보안 기술 관련 연구 개발을 지원할 것이라는 계획을 밝혔다. 이를 위해 사이버보안 전문인력을 양성하고자 초등학교, 대학교 등 학교 교과과정과의 연계 및 가능한 폭넓은 인재 풀을 형성하도록 사이버보안 경력자들의 경력단절을 막기 위한 직업경로를 개발하는 등 단순한 인력 양성이 아닌 전문성과 사후관리에도 집중을 하겠다는 계획을 밝히고 있다. 더불어 개방대학을 통해 사이버보안 공개 온라인 과정을 개발, 다수의 학생들을 대상으로 사이버보안에 대한 인식을 제고할 수 있도록 하였다. 이 밖에도 내무부 등 정부부처의 페 이스북을 활용한 일반 대중들의 사이버보안 인식 제고 노력도 함께 진행하고자 하였다.

5. 결론 및 시사점

영국은 국가차원의 지속성 있는 사이버보안 전략 추진을 위해 범부처 차원의 계획을 수립하고 추진해왔다. 특히, 효과적인 대응을 위해 전담부처외 민ᆞ군ᆞ국제기구와의 협력을 강화하는 등 다양한 이해 관계자들과의 협력을 중시하고 있다. 그리고 금융 등 국가 주요기반시설 대상의 사이버훈련 등을 통해 보안 강화를 위한 노력도 살펴볼 수 있었다. 그리고 사이버 보안에 대한 기술능력을 구축하고 인재를 양성하는 한편 관련 산업을 육성하기 위해 노력해 오고 있다. 또한, 영국 사이버보안 가치를 전파하기 위해 국제회의에 적극적으로 참여하여 영국의 입장을 전파하는 등 국제 사이버보안 정책과 전략을 선도하려는 노력을 기울이고 있는 것으로 파악되었다. 이러한 노력은 분명 국내 사이버보안전략을 추진하는데 있어 많은 참고사항이 될 것이다.

Contents

I. **Basic Overview of Information Security and Cybersecurity………………….. 13**

1. Information security
2. Cyber Security
3. Law and Regulation
4. Information Security culture

**II. ICT status in the UK ………………………………………………………..………………….. 21**

1. Major Ministires
2. Information protection environment
	1. UK`s ICT Development Index
	2. The history of Telecommunication in the UK
	3. Infrastructure
	4. Services
3. Information Protection Market Status

**III. UK`s Strategy for cyber security (2016~2020)…..……….……………….………. 40**

1. Background
2. The Scope of the strategy
3. Strategic Context
	1. Threats
	2. Vulnerabilities
	3. Conclusions
4. National Response to Cyber Criminal
	1. Visions
	2. Principles
	3. Roles and Responsibilities
5. Implementation

5.1. Defend

* 5.2. Protecting Government
* 5.3. Changing Public and Business Behavious.
* 5.4. Managing Incidents and Understanding the Threat.

6. Develop

 6.1. Strengthening Cyber Security Skills

 6.2. Stimulating Growth in the Cyber Security Sector

 6.3. Promoting Cyber Security Science and Technology

 6.4. Effective Horizon Scanning

# **I. Basic Overview of Information Security and Cybersecurity**

## 1. Information security

Information security (sometimes shortened to infosec) is a way to protect information by mitigating information risk. It is part of information risk management. This generally includes preventing or reducing the possibility of unauthorized/improper access to data, or the use, disclosure, interruption, deletion, corruption, modification, inspection, record or devaluation of illegal information. It also includes measures to reduce the adverse effects of such accidents. Protected information can be, for example, electronic or physical, tangible (eg documents) or intangible (eg knowledge). The primary focus of information security is to balance the confidentiality, integrity and availability of data (also known as the CIA triad) while maintaining a focus on effective policy implementation without compromising organizational productivity. This is mainly achieved through the following structured risk management process.

• Identify information and related assets, potential threats, vulnerabilities and impacts.

• risk assessment;

• Decide how to address, prevent, mitigate, share or accommodate risk.

• If risk mitigation is required, select or design appropriate security controls and implement them.

• Activity monitoring, adapting as needed to address issues, changes and opportunities for improvement.

To standardize this discipline, academia and experts collaborate to provide guidelines, policies and industry standards on passwords, antivirus software, firewalls, encryption software, legal responsibility, security awareness and education, and more. This standardization can be further strengthened by various laws and regulations that affect how data is accessed, processed, stored, transmitted and destroyed. However, if a culture of continuous improvement is not adopted, the implementation of all standards and guidelines within the enterprise may have limited impact.

### 1.1. Definition

Various definitions of information security summarized from various sources are given below.

1. "preservation of confidentiality, integrity, and availability of information. Note: It may also include other attributes such as reliability, accountability, denial and reliability." (ISO/IEC 27000:2009)

2. "Protect against unauthorized access, use, disclosure, interruption, alteration or destruction of information and information systems to provide confidentiality, integrity and availability" (CNSS, 2010)

3. "Only authorized users (confidentiality) have access to accurate and complete information (integrity) when necessary (ISACA, 2008)."

4. "Information security is the process of protecting an organization's intellectual property" (Pipkin, 2000)

5. "...Information security is a risk management area and is responsible for managing the costs of information risk to the business." (McDermott and Geer, 2001)

6. "A well-known conviction that information risk and control are balanced" (Anderson, J, 2003)

7. "Information security is information protection and minimizes the risk of information disclosure to unauthorized parties" (Bender and Eloff, 2003)

8. "Information security is an area of multidisciplinary research and professional activities related to the development and implementation of security mechanisms for all types (technology, organization, human orientation and legal) available to keep information in and out of all locations (in and out of the confines of the organization). As a result, the information system in which information is created, processed, stored, transmitted and destroyed is free from threats. Threats to information and information systems can be classified and security objectives can be defined for each category of threat. A set of security objectives identified as a result of threat analysis should be periodically modified to ensure compliance and suit evolving environments. Currently, the relevant set of security objectives may include confidentiality, integrity, availability, privacy, reliability and reliability, non-denial, accountability and auditability.(Cherdantseva and Hilton, 2013)

9. Securing information and information resources using a communications system or device means protecting information, information systems or books from unauthorized access, damage, theft or destruction (Curo and Ross, 2010).

## 2. Cyber security

Computer security, cybersecurity, or information technology security (IT security) is the protection of computer systems and networks from theft or damage of hardware, software or electronic data as well as from the interruption or misdirection of services they provide.

The field is becoming more important due to the growing reliance on wireless network standards such as computer systems, the Internet and Bluetooth and Wi-Fi, and the growth of "smart" devices, including various devices that make up smartphones, televisions and the Internet of Things. Because of its complexity, both in politics and technology, cybersecurity is also one of the major challenges in the modern world.

## 3. Law and Regulations

Below is a partial listing of governmental laws and regulations in various parts of the world that have, had, or will have, a significant effect on data processing and information security. Important industry sector regulations have also been included when they have a significant impact on information security.

* The UK Data Protection Act 1998 makes new provisions for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. The European Union Data Protection Directive (EUDPD) requires that all E.U. members adopt national regulations to standardize the protection of data privacy for citizens throughout the E.U.
* The Computer Authority Act 1990 is a law that the British Parliament defines computer crime (e.g., hacking) as a crime. The law has become an inspiration model for several other countries, including Canada and Ireland, when they later draw up their own information security laws.

## 4. Information security culture

The information security culture is more than just describing the state of security-aware employees, it is the organization's ideas, customs, and social behaviors that affect information security in a positive and negative way. Cultural concepts can make various parts of an organization work effectively or interfere with the effectiveness of information security within an organization. The way employees think and feel about security and the actions they take can have a major impact on an organization's information security. Roer & Petric (2017) identifies seven major dimensions of information security culture in organizations.

* Attitude: Employee feelings and emotions about various activities related to the organization's information security.
* Behavior: actual or intended activities and risk-taking behaviors of employees that directly or indirectly affect information security.
* Awareness: Employee perceptions, verifiable knowledge and beliefs about practices, activities and self-efficacy relationships related to information security.
* Communication: How employees communicate with each other through affiliation, security issues support, and incident reporting.
* Compliance: The ability to comply with an organization's security policy, recognize the existence of the policy, and remind the content of the policy.
* Norms: Awareness of the behaviors and practices of security-related organizations, which are informally considered by employees and colleagues (e.g., written expectations about hidden expectations for security behaviors and the use of information and communication technologies).
* Responsibility: It plays an important role in helping employees understand the organization's roles and responsibilities by maintaining or threatening information security.

Andersson and Reimers (2014) found that employees often do not see themselves as part of an organization's information security "effort" and take steps to ignore the best interests of the organization's information security. Research shows that the information security culture needs to be constantly improved. From the information security culture to analysis to change, the author said, "After all, the process, evaluation and change or maintenance cycle is never over." To manage the information security culture, you need to perform 5 steps: pre-assessment, strategic planning, operational planning, implementation and post-assessment.

* Pre-assessment: Understand employee perceptions of information security and analyze current security policies.
* Strategic planning: To create a better awareness program, you need to set clear goals. It is helpful to gather people.
* Operation plan: Foster a good security culture based on internal communication, management purchasing, security awareness and training programs.
* Implementation: Must be characterized by commitment to management, communication with organizational members, processes and employee commitments to all members of the organization.
* Ex post evaluation: better measure the effect of the previous step and continuously improve it

# **II. ICT status in the UK**

**1. Major ministries**

Britain's cybersecurity strategy is centred around the Cabinet Office. The Cabinet is in charge of coordinating information protection activities and work for government agencies, while the National Cyber Security Center provides advice and support to the public and private sectors on how to avoid computer security threats.

### 1.1. National Cyber Security Centre

The National Cyber Security Center (NCSC) is a British government agency that provides advice and support to the public and private sectors on how to avoid computer security threats. Its London-based operation began in October 2016, and its parent organization is GCHQ.

The NCSC has absorbed and replaced cyber-related responsibilities of CESG (Information Security Arm of GCHQ), Cyber Assessment Centre (CCA), Computer Emergency Response Team UK (CERT UK), and National Infrastructure Protection Center (CPNI). It was built on the basis of the initial efforts of these agencies and the Cabinet to provide guidance on information security for the wider private sector in the UK, such as the "10-Step" guidance issued in January 2015. In a pre-launch announcement, the British government said the NCSC will first work with the Bank of England to advise financial institutions on how to strengthen their online defences.

The center was first announced by Finance Minister George Osborne in November 2015. The existing GCHQ cyber director Xia Lan Martin is leading the new center, and Dr. Ian Levy, currently director of cybersecurity technology at GCHQ, has taken the same role in the NCSC. A detailed paper on the creation of the NCSC, including a description of the structure and future tasks of the NCSC written by then GCHQ Director Robert Hannigan, who contributed greatly to the establishment of the center, was published by the Royal United Services Institute in February 2019.

The center was dedicated by the Queen on February 14, 2017. Treasury Secretary Philip Hammond announced plans to invest 1.9 billion pounds and send 100 industry figures to the NCSC.

In April 2016, the Ministry of National Defense announced that the Cyber Security Operations Center (CSOC), with a budget of more than 40 million pounds, was "to protect the ministry's cyberspace from malicious actors." It is located in MoD Kosham.

In October 2017, technology director Ian Levy was targeted by email naughty James Linton for a fake industrial event, but Levy correctly identified an unexpected header and opened a security blog about the incident with him.

### 1.2. Cabinet Office

The Cabinet Office is the department of the British government in charge of supporting the British prime minister and cabinet. It consists of various units supporting the State Council and coordinating the delivery of government objectives through other departments. There are currently just over 2,000 employees, most of whom work in Whitehall. Employees working in the Prime Minister's Office belong to the Office for Government Policy Coordination.

The department was formed in December 1916 in the Secretariat of the Imperial Defence Commission under the leadership of the first cabinet minister, Sir Maurice Hanki.

Traditionally, the most important part of the role of the Office for Government Policy Coordination has been to promote collective decision-making by the Cabinet through the operation and support of committees at the Cabinet-level. This is still the main role, but since some functions of the Ministry of Civil Affairs were absorbed in 1981, the Office for Government Policy Coordination has also helped push for a broad range of ministerial priorities throughout Whitehall.

There are also miscellaneous units that cannot sit well in other departments. For example:

* The history section was established in 1906 as part of the Imperial Defence Commission and is related to official history.
* The Joint Intelligence Committee was established in 1936 and transferred to the department in 1957. It commands Britain's national intelligence agency and deals with intelligence assessments.
* The ceremonial division was established in 1937 and transferred to the department in 1981. It was originally associated with all the ceremonial functions of the state, but today it handles courtesy and appointment.

In modern times, the Cabinet is often responsible for the policy sector, which is the priority of the government of the time. Departments managing these areas come in and out of the Office for Government Policy Coordination as government priorities (and governments) change.

## 2. Information Protection Environment

Britain has long been recognized by the IRA's struggle for independence and terrorist acts for the need to strengthen the information protection industry and services.

• It also forms the third-largest market in the world after the United States and Japan, and the largest market for information protection in the EU in the past.

• Multilingual societies, as well as the information security market, are forming a multilingual society, and a multilingual population from the British Commonwealth is also forming. Due to social unrest, CCTVs installed to prevent crimes such as theft and terrorism are the largest in the physical security market in the past, indicating that demand for security equipment is very high.

Along with the announcement of national cybersecurity strategies, the British government also announced strategies to protect cyber attacks in each industry, including essential and new industries, to drive the development of cybersecurity.

 • Under the National Cyber Security Initiative announced in 2016, 1.9 billion pounds (2.7 trillion won) was invested in cybersecurity and the National Cyber Security Center (NCSC) and London's RORCA (London Office for Rapid Cyber Security Innovation) was established to foster cybersecurity personnel and support projects.

 •Necessary service providers should implement effective cybersecurity measures to ensure that essential networks and infrastructure are secure, resilient and that new fines can be imposed if insufficient.

 • The Department of Transportation has issued guidelines on cybersecurity for connected cars and self-driving cars, providing consistent security policies to all stakeholders involved in the manufacturing supply chain.

Recently, investments in software such as precision electronics and information security solutions to enhance the safety of cyberspace have also been increasing.

 • The Prime Minister's Office is actively pursuing investment strategies for the establishment of national cybersecurity systems to strengthen information protection activities, especially cybersecurity activities.

 • As Britain is also not free from countries subject to violent Middle East violence, such as Islamic State (IS) and al-Qaida, it is inevitable to strengthen intelligence security activities to prevent their movement, illegal entry control, and solidarity with Islamic forces in Britain through cyberspace. Or it could be a terrorist sabotage.2. Internet and Communication Environment

### 2.1. UK`s ICT Development Index

The UK continues to improve its information and communication environment by investing 1 billion pounds to install broadband infrastructure across the country and 400 million pounds to achieve 1GB/S Internet speed, with the ITU's ICT Development Index rising from 10th in 2010 to 5th in 2016.

 The British government's recent nationwide high-speed broadband deployment project has led to a surge in Internet downloads and significant improvements in access and utilization of information and communications to the general public.

 However, the ICT sector (technology) ranked 29th as of 2016, lower than other sectors, requiring the government's policy efforts to strengthen it.

### 2.2. The history of Telecommunication in the UK

National Telephone Company (NTC), a British telephone company from 1881 to 1911, gathered small local companies in the early stages of the telephone. It was acquired by the General Post Office (GPO) in 1912 under the Telephone Transmission Act of 1911.

By 1982, Britain's main private communications system was a state monopoly system known as Post Office Communications. Radio and television broadcasts were monopolies of the BBC and the Independent Broadcasting System (IBA). The two agencies controlled all broadcasting services, and directly owned and operated broadcasting transmitter sites. Cell phones and Internet services did not exist at that time. The monopoly of private communications ended with the arrival of Mercury Communications in 1983. The post office system developed into British Telecom and was privatized in 1984. Broadcasting transmitters belonging to the BBC and the IBA were privatized in the 1990s and now belong to Babcock International and Arqiva.

British Rail Telecommunications was created by British Rail (BR) in 1992. It was Britain's largest private communications network, consisting of 17,000 kilometers of optical fiber and copper cables that connect all major cities and towns in the UK and provide a network of connections to the European continent through channel tunnels. BR also operated its own cross-country wireless network that provided dedicated cross-train mobile communication, and in the early 1980s BR helped establish the current C&WC core infrastructure, Mercury Communications, by building a resilient 'eight-shaped' fiber network on British railway lines across London, Bristol, Birmingham and Reed.s and Manchester

During the same period, telecommunications regulations have changed many times, and most agencies have been merged into Ofcom, an independent regulator and rival agency of the British telecommunications industry.

### 2.3. Infrastructure

**Domestic Daytime Infrastructure**

All communication trunks are now digital. Most are carried over the national fibre optic network. There are several companies with national fibre networks, including BT, Level 3 Communications, Virgin Media, Cable & Wireless, Easynet and Thoe. Microwave links are used up to 155 Mbit/s levels, but are rarely cost effective when the bit rate is high.

**international trunk**

Britain is the focal point of many of the world's undersea communication cables, which are now mostly digital fiber-optic cables. There are also many satellite links, but they now provide a relatively small portion of international bandwidth.

**broadcast transmission**

The BBC and most commercial broadcasting organizations lease transmission facilities from one or more transmission companies. The main exception is small local radio stations. Some radio stations find it more cost-effective to provide their own radio stations.

**fixed telephone line**

BT is still a major provider of fixed telephone lines, both POTS and ISDN, and it has a universal service obligation, although companies can now contract Openreach to install phone lines on their behalf, rather than ordering customers to install them and then hand them over. Virgin Media is the second-largest company in the residential telephone line market. Other companies also offer fixed telephone lines, but mainly to large corporations in major cities.There are many other providers who sell fixed telephone services carried over BT lines. They have no network infrastructure of their own.

**Mobile phone network 4th generation network**

Long-term evolution (LTE) service is currently being released. EE started the 4G network in October 2012, using part of the existing 1800 MHz frequency. O2 and Vodafone will use 800MHz band with Vodafone and 2,600MHz band will also be used for service. O2 started its 4G network in London, Leeds and Bradford on August 29, 2013, with 13 additional cities added by the end of 2013. Vodafone launched the 4G service on August 29, 2013, and initially, 12 cities were to be added by the end of 2013 in London. The three countries launched LTE services in London, Birmingham, Manchester, Reading, Wolverhampton and Black Country in December 2013. The full rollout for the rest of the subscribers was initiated step by step on 5 February 2014 with automatic SIM updates. By the end of 2014, more than 50 cities and more than 200 villages will receive LTE coverage. 3 was not available until October 2013 under the condition that part of the 1800 MHz spectrum of EE was acquired for 4G use.

### 2.4. Services

**Fixed telephone**

There were 35 million (2002) central line telephones in Britain. Telephone services in the UK were originally provided by private enterprises and local city councils, but by 1912–13 [12], all services were bought by the General Post Office, except telephone services in Kingston on Hull, Yorkshire and Guernsey. Postal Service Telephone also operated telephone services on Jersey and Manseom Island until 1969, where the islands assumed responsibility for their postal and telephone services.

Post office telephony was reorganized into British Telecom (or BT) in 1980–81 and was the first state-owned industry privatized by the Conservative Government. The Hull Telephone Department was sold by the Hull City Council to Kingston Communications in the late 1990s, marking the 100th anniversary of its foundation in 2004.

**Mobile telephones**

There are more mobile phones than people in the UK. In 2011 there were 82 million subscriptions in the UK. There were 76 million in 2008 and 55 million in January 2005. Each of the main network operators sells mobile phone services to the public.

**Numbering**

Telephone numbers in the UK have a set numbering plan regulated by the Ofcom, which replaced the Office of Telecommunications (Offel) in 2003. Each number consists of an area code (one for large cities and one for urban and surrounding environments) and a subscriber number (personal number). Mobile IMSI is the actual number assigned to the mobile phone number and provides the MNO with individual licenses.

**television and radio broadcasting**

**Radio**

In 1998, there were 663 radio stations: 219 in the morning, 431 in FM and three short waves. Radio receivers reached 84.5 million sets (1997). Today there are about 600 licensed radio stations in Britain.

**Television**

In 1997, 30.5 million households had televisions.

Analogue television broadcasting stopped in Britain in 2012 and was replaced by digital ground service previews that operate through DVB-T and DVB-T2 standards (for HD broadcasting). Digital Satellite is provided by BSkyB (subscription and free service) and Freesat (only air service free) at 28.2° east. Digital cables are mainly provided by Virgin Media.

**Internet**

The top-level domain of the country code for British web pages is .uk. The British Nominet is .uk. Network information centres and secondary domains should be used.

52% (1.26 million households) of households reported Internet access at the end of 2004 (Source: Statistics Korea omnibus survey). Broadband connectivity accounted for 50.7% of all Internet connections in July 2005, with one broadband connection being created every 10 seconds.[16] Broadband connectivity increased by nearly 80% in 2004. In 1999, there were 364 Internet service providers (ISPs). Public libraries also offer Internet access sometimes for a fee.

In 2017, 90 per cent of households have Internet access. The ratio increased from 80 per cent in 2012 and 61 per cent in 2007.

## 3. Information Protection Market Status

### 3.1. Market Overview and Scale

 **Britain has traditionally developed around the physical security market.**

• Britain has traditionally been plagued by bombings in the Republic of Ireland and has recently suffered terrorist attacks and black riots by Islamic terrorists, and over the past few years, the level of terrorism committed by far-right groups has been increasing, leading to advances in physical security.

• In November 2018, as part of the national surveillance camera strategy, the British government issued in-house monitoring guidelines as a demonstration of the standards for CCTV operations before applying them to the entire CCTV industry.

• In-house monitoring guidelines provide minimum requirements for the safe management of public CCTV systems

• Follow-up updates to the code of conduct for surveillance cameras announced in 2013 include the Buyer Toolkit, the Public CCTV System Implementation Compliance Certificate, Self-Assessment, and the Impact Assessment of Information Protection in 2018.

 Britain's Homeland Security spending will be allocated to the need for border security, defending against cyberattacks and threats from terrorist organizations. Britain's role in Afghanistan, Iraq and North Africa is highly exposed to terrorism, and it is also in a border dispute with Spain over Spain's demand for the return of Gibraltar on the Gibraltar border. The external leakage of detailed information on 600,000 foreign visitors collected in March 2018 as e-Borders13 highlighted the need to reorganize the pre-Brexit IT systemOctober 2018 London Heathrow Airport introduced a facial recognition system to enhance passenger comfort and enhance security

The British government wants to install full-body scanners, boarding pass scanners, etc. to defend terrorist groups upon arrival at all airports in the UK in the near future. However, there are concerns about the inaccuracy of the facial recognition system, legal management, and poor supervision.

Strengthen the protection of national security-related industries. The British government publishes a White Paper on National Security and Investment to give the British government the authority to pre-examine new projects that could threaten national security. If the acquisition is more than 만70 million or the market share is more than 25% after mergers and acquisitions (as part of the Act was amended in June 2018), military technology (or military and military weapons manufacturing) and computer hardware. If more than 25% of the entire entity's shares are acquired by a trigger event that triggers government intervention, the entity may exercise significant influence or control, and if it gains additional significant influence or control after the above situation, the government may exercise its right to take over 50% or more of its assets in advance.

Excluding Huawei's 5G network products in the area of cybersecurity. In July 2018, the Huawei Cyber Security Evaluation Centre in the UK released a report pointing to the security issues of Huawei's 5G network products. A report by the Huawei Cyber Security Assessment Center in the UK suggests cyberattacks penetrating through back doors in the network, pointing to the security issues of Huawei's products. According to CVE Detail, a security vulnerability statistical and analysis site, as of June 2018, there were 152 security vulnerabilities revealed in Huawei products, which is equivalent to the total of 157 security vulnerabilities in 2017.

**UK 12th in ITU Global Cybersecurity Index.**

According to the ITU's November 2017 Cybersecurity Index data, the UK is one of the 12th-ranked countries in the world, ahead of Korea (13th), followed by Estonia, France and Norway in Europe. In particular, the government has been strengthening national information protection policies to prevent infiltration attacks and terrorism through cyberspace, and the demand for related devices, solutions, and software will continue to increase. The UK's information protection market is highly competitive among global companies as it is highly likely to grow. The domestic information protection industry is also highly competitive among global information protection companies as much of their demand depends on imports. While high-priced precision products are a big part of the U.S., low- and medium-priced physical security products are made in China with price competitiveness.

 **Cybersecurity Start-ups stand out**

UK cybersecurity startups focus on identity and access management, information security and collaboration. Demonstrates the soundness of the cybersecurity market in that it is spread evenly across all industries in the area of entry into cybersecurity startups. The growth of such UK cybersecurity startups is backed by increased investment agreed with universities with great interest from the UK government. Underscoring the importance of security in new industries and new products in the UK where ICT technology is integrated. Implement the Automatic and Electric Vehicle Act, which imposes liability on insurance companies for self-driving cars and smart cars. The British government will conduct a three-year law review with the aim of commercializing autonomous vehicles by 2021, invest 22 million pounds in 22 technology research projects related to autonomous vehicles, and invest a total of 1 billion pounds in autonomous vehicles and eco-friendly vehicles. In March 2018, the UK National Cyber Security Center announced guidelines for Internet-connected products such as IoT and IP cameras. The guidelines include strengthening security measures, including setting a unique default password for the product to be released. However, the problem exists that it is not legally binding and therefore ineffective.

According to data from the British Department of Digital Culture, Media and Sports, 846 companies operate in the UK cyber security market and its sales are estimated at 5.6 billion pounds. The British government will announce a new five-year strategy in 2016 and invest approximately $2.4 billion in cybersecurity defence and readiness over the next five years, including the new National Cybersecurity Centre. According to International Trade Management Data19 of the U.S. Department of Commerce, it is worth about $5 billion and is also the largest and most concentrated market in Europe. 73% of UK large enterprises experienced cyber attacks and breaches in 2017.

UK damage from cybercrime is estimated at $3 billion. The EU General Data Protection Regulations (GDPRs) are expected to facilitate spending on cybersecurity by mandating infringement reporting and imposing heavy fines of 4% or up to $25 million in global sales for severe data loss.

< UK cyber security market (2017) > (Unit: Million £)



\*Source: Cyber security market size in the UK from 2010 to 2017

RSM analysis estimates that Britain has a workforce of 31,300 to 40,000 people. The revenue generated per person is 181,000 won and 75,000 won per person. Most enterprises are distributed in the areas of network security, information risk assessment and management, and cyber professional services.

Collaboration between cybersecurity companies and insurance companies is underway, with insurance company Lloyd's (London) offering discounts to companies that use software from cybersecurity company Tripwire, while clearing IP addresses jointly implemented by insurance company AIG and cyber security company Invicta Network.

There is a lack of prior research in the existing cyber insurance sector. In 2016, Frost & Sullivan conducted an analysis of the defense and security industries, including cyber insurance.

According to data from the Institute for Homeland Security in May 2017, Britain's national security and public safety sectors are expected to grow 11.3 percent annually between 2015 and 2020.

Britain faces far broader security challenges than economic ones, and there are no signs of a decline in terrorist threats by extreme Islam.

According to the UK Institute of Homeland Security Market Research, the 2015-2020 market will grow at an average annual rate of 11.3%, four times larger than the previous average growth rate of 2-3% in the 2010-2015 period.

This market growth involves strengthening the entry and exit of homeland security and the public safety market, and products and services are expected to double or triple, although there are currently business opportunities in similar areas.

# III. UK`s Strategy for cyber security (2016~2020)

## 1. Background

Information and communication technology has evolved over the past two decades and is now integrated into virtually every aspect of our lives. Britain is a digitized society. Our economy and everyday life are richer than that.

The changes caused by this digitization create new dependencies. Our economy, government administration, and the provision of essential services are now dependent on the integrity of cyberspace and the infrastructure, systems and data that support it. The loss of trust in its integrity would jeopardize the benefits of this technological revolution.

To facilitate this interconnected digital environment, much of the hardware and software was originally developed with priority on efficiency, cost and user convenience, but security was not always designed from the ground up. Malicious actors (hostile states, criminal or terrorist organizations, individuals) can exploit the differences between convenience and security. Closing the gap is a national priority.

As the Internet extends beyond computers and mobile phones to other cyber-physical systems or "smart" systems, the threat of remote attacks is expanding with a number of new technologies. Power systems, air traffic control systems, satellites, medical technology, industrial plants, traffic lights, etc. The systems and technologies that support our daily lives are potentially vulnerable to interference because they are connected to the Internet.

In 2015, the National Security Strategy (NSS) reaffirmed cyber threats as a first-stage risk to UK interests. The National Security Council (NSS) has resolved the government's determination to combat cyber threats and "take strong and innovative measures as a global cyber security leader." This national cybersecurity strategy fulfills that promise.

In preparing this new strategy, the government is based on the performance, goals and judgments of the first five-year national cybersecurity strategy announced in 2011. The government invested 860 million pounds during that period and was proud of what was achieved. Policies, institutions and initiatives developed over the past five years have helped the UK to become a leading global company in cybersecurity.

These are solid foundations. But the continuity and originality of those who will threaten us, and the spread of gaps in our fragility and abilities and defenses mean that we have to work harder to combat the threat. A comprehensive approach is needed to effectively secure cyber interests. Our commitment to further investment and intervention is based on the following assessment.

• The magnitude and dynamic nature of cyber threats, and our vulnerability and dependence, means that maintaining our current approach is not enough to keep us safe.

• The market-based approach to promoting cyber hygiene is as follows.

Because it has not been able to calculate the speed and scale of the necessary changes, governments need to lead the way and engage more directly by influencing and providing resources to combat cyber threats.

• The government alone cannot provide all aspects of national cybersecurity. We need a built-in, sustainable approach where citizens, industry and other social and government partners play a full role in network, service and data security.

• The UK needs a vibrant cybersecurity sector and a supporting technology base to keep pace and stay ahead of changing threats.

**2. The Scope of strategy**

This strategy is intended to shape government policies while presenting a consistent and persuasive vision that can be shared with the public and private sector, civil society, academia and a wider population.

The strategy covers the entire UK. The UK government will ensure that this strategy is implemented against:

All regions of the UK will work closely with the delegated governments on their application to Scotland, Wales and the North, as far as mandates are concerned.

Ireland (respects three separate legal jurisdictions and four educational systems in the UK). If the proposals presented in the strategy involve issues delegated, their implementation will be appropriately agreed with the appropriate government in accordance with the transfer solution.

The strategy offers action that is proposed or recommended for all sectors of the economy and society, from central government departments to leaders across industries and individual citizens. This strategy aims to increase cybersecurity at all levels for our collective benefit, and will be the basis for the UK's international participation to promote good Internet governance.

In this strategy,'cyber security' refers to protecting information systems (hardware, software and related infrastructure), data about them, and the services they provide from unauthorized access, harm or misuse. This includes risks intentionally caused by system operators or accidentally due to failure to follow security procedures.

Consistent with the assessment of the challenges we are facing for the performance of our 2011 strategy, this document provides:

• An updated assessment of the strategic context, including the threats that are evolving today, the ones that pose the most serious threat to our interests, and the tools they can use at will.

• Vulnerability review and vulnerability development method over the past 5 years

• The government's vision for cybersecurity in 2021 and its key objectives to achieve it (including guiding principles, roles and responsibilities, and the way and place of government intervention).

• How to implement the policy: Set up a government-led place and place where you expect to be able to cooperate with others.

• How you want to assess progress toward your goals

**3. Strategic context**

When the last National Cyber ​​Security Strategies was announced in 2011, the magnitude and impact of technological change were already evident. The trends and opportunities described at that time have since accelerated. New technologies and applications have emerged, and the greater influx of Internet-based technologies, especially in developing countries, has increased opportunities for economic and social development. These developments will or will bring significant benefits to connected societies like us. However, as our reliance on networks in the UK and abroad increases, so are the opportunities for people to compromise our systems and data. Likewise, geopolitical terrain has changed. Malicious cyber activities don't know international boundaries. State actors are experimenting with aggressive cyber capabilities. Cybercriminals are expanding their efforts and expanding their strategic methods to obtain higher value rewards from UK citizens, organizations and institutions. Terrorists and their sympathizers are attacking at a low level and are eager to do more important things. This chapter describes the nature of these threats, their vulnerabilities, and how they continue to evolve.

### 3.1. THREATS

**Cyber criminals**

This strategy deals with cybercrime in relation to two interrelated forms of criminal activity.

• Cyber Dependent Crime – A crime that can only commit crimes using information and communication technology (ICT) devices. Here, the device is both a tool for committing crime and a target for crime (e.g., developing and spreading malicious programs). Hacking to steal, damage, distort or destroy financial interests, data and/or networks or activities) and

• Cyber-assisted crimes – Traditional crimes that can be scaled up or reached using computers, computer networks, or other forms of ICT (such as cyber-assisted fraud and data theft).

 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.

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.

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.

**States and state-sponsored threats**

We focus on government, defense, finance, energy and telecommunications sectors, and regularly see state and government sponsored organizations attempt to penetrate the UK network for political, diplomatic, technological, commercial and strategic advantages.

The capacity and impact of these main cyber programs vary. Most developed countries continue to improve their capabilities at speed while integrating encryption and anonymization services into their tools to maintain confidentiality. Although it has the technical ability to deploy sophisticated attacks, the victims' defenses are often weak, so they can often achieve their goals using basic tools and techniques for vulnerable targets.

Few states have the technical ability to pose a serious threat to Britain's overall security and prosperity. However, many other states are developing sophisticated cyber programs that could threaten UK interests in the near future. Many states that want to develop cyber espionage capabilities can purchase computer network access tools'on the fly' and change their use to spy.

Beyond espionage threats, a small number of hostile foreign threat actors have developed and deployed aggressive cyber capabilities, including destructive cyber capabilities. This capability threatens the security of important UK infrastructure and industrial control systems. Some countries may use this ability to violate international law with the following beliefs:

They can do so with relative punishment, encouraging others to follow. While destructive attacks are rare worldwide, they are increasing in number and impact.

**Terrorists**

Terrorist groups are eager to continue harmful cyber activities against the UK and its interests. Currently, the technology of terrorists is considered low. Nevertheless, so far the impact of low capacity activities on the United Kingdom has been disproportionately high: simple defense and boxing activities (if hacked personal information is'spilled online') have attracted media attention from terrorist groups and their supporters. It can threaten their victims.

The current assessment is that physical terrorist attacks, rather than cyber threats, will remain a top priority for terrorist groups. As more and more computer illiterate generations fall into extremism and exchange potentially advanced technology, we are planning a greater amount of low-difference (DDS) destruction activities for the UK. The likelihood that many skilled extremist lonesome actors will emerge will also increase, and the risk that terrorist organizations will try to recruit ready-made insiders will also increase. Terrorists will use any cyber abilities to get the best possible effect. Thus, even a moderate increase in terrorist capabilities can pose a significant threat to the UK and its interests.

**Hacktivists**

The Hackativist group is decentralized and issue-oriented. They set and select goals in response to perceived complaints, and incorporate the quality of vigilantes into many of their actions. While most hackytiv cyber activities are inherently destructive, more capable hackytivists have been able to do more and more damage to their victims.

**Script Kiddies**

So-called'script kiddies'-In general, less skilled individuals who conduct cyber attacks using scripts or programs developed by others are not considered to pose a real threat to the wider economy or society. However, they have access to hacking guides, resources and tools on the Internet. Because of the vulnerabilities found in Internet-facing systems used by many organizations, the actions of'Script Kiddy' can sometimes disproportionately damage the affected organizations.

### 3.2. VULNERABILITIES

**An expanding range of devices**

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.

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.

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**

The perception of software and network technical vulnerabilities and the need for cyber hygiene in the UK has undoubtedly increased over the past five years. This is partly due to the public's increased awareness of key cyber events affecting governments and businesses, as well as the result of initiatives such as the government's '10 steps to cyber security'. Cyber ​​attacks are not necessarily sophisticated or inevitable, and are often the result of vulnerabilities that can be easily corrected and prevented. In most cases, the decisive factor in the success of cyber attacks continues to be the vulnerability of the victim rather than the originality of the attacker. Companies and organizations decide where and how to invest in cybersecurity based on cost-benefit assessments, but ultimately are responsible for the security of their data and systems. Only by fully investing in people, technology and governance, and by balancing the risks of sensitive systems and sensitive data arising from cyberattacks, companies will be able to reduce their exposure to potential cyber hazards.

**Insufficient training and skills**

We lack the skills and knowledge to meet our cybersecurity needs across the public and private sectors. In the business, many employees are unaware of cybersecurity, and partly because of the lack of formal training, they do not understand their responsibilities in this regard. The public is also insufficient cyber awareness.

We also need to develop expertise and capabilities to keep pace with rapidly evolving technologies and manage related cyber risks. This technological gap represents a national vulnerability that must be addressed.

**Legacy and unpatched systems**

Many UK organizations will continue to use vulnerable legacy systems until the next IT upgrade. The software of these systems often relies on older, unattached versions. These older versions often suffer from vulnerabilities with tools that attackers can find and use. An additional problem is the use of some software organizations that do not have a patch system.

**Availability of hacking resources**

Hacking information and user-friendly hacking tools are available on the Internet, making it possible for people who want to develop hacking abilities. The information that hackers need to successfully compromise victims is often publicly accessible and can be quickly gathered. Everyone from the living room to the boardroom needs to know how much of their personal information and systems are exposed to the Internet and how vulnerable they are to vulnerable cyber attacks.

### 3.4. CONCLUSIONS

Britain has been pursuing policies and founding agencies that have strengthened our defenses and mitigated some of the threats we face in cyberspace. However, it is not yet ahead of the threat. Despite the rapid increase in the amount of malicious code and the number of such malicious actors, the types of malicious cyber actors we have to face and their motivation have largely withstood. The skills of the most technologically advanced enemies, a select number of states and elite cybercriminals, have grown. Our collective challenge is to make our defenses evolve and respond agile enough to respond, reducing the ability of malicious actors to attack us and addressing the root cause of the vulnerability described above.

**4. National response to cyber criminals**

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.

### 4.1. VISION

Our vision for 2021 is that the UK is safe and resilient to cyber threats, thriving and confident in the digital world.

To realize this vision, we will strive to achieve the following goals.

• Defense We have the means to defend the UK from evolving cyber threats, respond effectively to incidents, and ensure that UK networks, data and systems are protected and resilient. Citizens, businesses, and the public sector have the knowledge and ability to defend themselves.

• The UK will be a strong target for all forms of cyberspace invasion. We track, prosecute and prosecute criminals, detecting, understanding, investigating and interfering with hostile behavior. We have the means to take aggressive action in cyberspace.

• Development We have an innovative and growing cybersecurity industry supported by global scientific research and development. We have a self-sustaining talent pipeline that provides technology to meet our national needs across the public and private sectors. Our state-of-the-art analytics and expertise will enable the UK to meet and overcome future threats and challenges.

In support of these goals, we will exert influence by pursuing international action and investing in partnerships. We will shape the global evolution of cyberspace in a way that advances our broader economic and security interests.

### 4.2. PRINCIPLES

To achieve this goal, the government will apply the following principles.

• Our actions and policies will be driven by the need to protect our people and promote our prosperity.

• We will treat cyber attacks on the United Kingdom as seriously as conventional attacks that are equivalent to us, and we will defend ourselves as needed.

• We are expected to act in accordance with national and international law and expect others to do the same.

• We will strictly protect and promote our core values. These include democracy, rule of law, freedom, open and responsible governments and institutions, human rights, and freedom of expression.

• We will preserve and protect the privacy of British citizens.

• We will cooperate. Cooperation with all sectors, including the public sector, businesses, institutions, and individual citizens, ensures that the UK can be successfully secured in cyberspace.

• The government will fulfill its responsibilities and lead a national response, but businesses, organizations and individual citizens are responsible for taking reasonable steps to protect themselves online and ensuring that they remain flexible and consistent in the event of an event.

• Responsibility for the security of organizations across the public sector, including cyber security and online data and service protection, rests with each minister, standing office, and management committee.

• Businesses and organizations will not accept the significant risks to the people and the nation as a whole as a result of not taking the steps necessary to manage cyber threats.

• We will share our views and work closely with countries where our security overlaps, recognizing that cyber threats do not know the borders. We will also work extensively across a range of international partners to influence the broader community while recognizing the value of the broader coalition.

• To ensure that government interventions have a real impact on national cybersecurity and resilience, we seek to define, analyze and present data that measure success in achieving the state and strategic goals of collective cybersecurity.

### 4.3. ROLES AND RESPONSIBILITIES

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

**Individuals**

As citizens, employees and consumers, we take practical steps to secure assets that we value in the physical world. In the virtual world, we must do the same. In other words, we must take personal responsibility to take all reasonable steps to protect our hardware, ie smartphones and other devices, as well as data, software and systems that provide freedom, flexibility and convenience in our personal and professional lives. Means.

**Businesses and organisations**

Enterprises, public and private sector organizations and other institutions hold personal data, provide services, and operate systems in the digital domain. The link of this information revolutionized their operations. However, with these technological changes, they are responsible for protecting their assets, maintaining the services they provide, and integrating the appropriate level of security into the products they sell. Citizens, consumers, and society as a whole expect businesses and organizations to take all reasonable steps to protect their personal data and build resilience (resistance and resilience) to the systems and structures they depend on. Companies and organizations should also understand that if they are victims of cyber attacks, they are responsible for the consequences.

**Government**

The main task of the government is to protect the country from attacks by other countries, protect citizens and the economy from harm, protect our interests, protect basic rights, and establish a framework for domestic and foreign criminals to be judged by law.

As holders and service providers of sensitive data, governments take strict steps to provide safeguards for information assets.

The government also has an important responsibility to advise and inform citizens and organizations what they should do to protect themselves online, and if necessary, we must set standards that we expect major companies and organizations to meet. .

Although the core sector of our economy belongs to the private sector, governments are ultimately responsible for ensuring their national resilience and, with partners throughout the executive branch, are responsible for maintaining essential services and functions throughout the government.

**Driving change: the role of the market**

In 2011, the Strategic and National Cyber ​​Security Program sought to promote public and private sector performance and increase capacity by looking at the market to promote correct action. We expected commercial pressure and government-level incentives to ensure the right business investment in the right cyber security, to facilitate the flow of investment in our industry, and to promote the right technology pipeline for the sector.

Achieved a lot. Across the economy and the wider society, awareness of the risks and actions needed to mitigate cyber risk has increased over the past five years. However, the combination of market power and government encouragement itself was not enough to secure our long-term interests in cyberspace at the required rate. Too many networks, including critical sectors, are still unstable. The market is not properly assessing cyber risk, and thus is not properly managing cyber risk. Too many organizations still suffer from the most basic level of breaches. Too few investors are willing to take risks in supporting entrepreneurs in the field. Too few graduates and people with the right skills are coming out of the education and training system.

The market still has a role to play and in the long run it will have a bigger impact than the government can do. However, the rapidity of the threats faced by the UK and the increasing vulnerability of the digitized environment require greater action in the short term from the government.

**Driving Change: Expanding the Role of Government**

Therefore, the government must set the pace to meet the country's cybersecurity needs. Only the government has access to the information and other assets needed to defend the country from the most sophisticated threats.

Only the government can promote cooperation across the public and private sectors and ensure that information is shared between the two. The government plays a leading role in defining and implementing cybersecurity excellence in consultation with industry.

The government will bring significant improvements to national cybersecurity over the next five years. This ambitious and transformative program will focus on four broad areas:

• Lever and incentives. The government will invest to maximize the potential of the truly innovative UK cyber sector. We will do this by supporting startups and investing in innovation.” We will also seek to find and bring talent early in the education system and develop a clearer path into jobs that need better justice. It will also use all available levers, including the upcoming General Data Protection Regulations (GDPR), to increase cybersecurity standards across the economy when needed through regulation.

* Expanded information focused on threats and law enforcement agencies Information agencies, the Ministry of National Defense, the police and the National Police Agency cooperate with international partners to expand efforts to identify, predict and disrupt hostile cyber activities of foreign actors, cyber criminals and terrorists. Will do. This will improve their intelligence gathering and exploitation with the goal of proactively acquiring information about the intentions and abilities of our enemies.
* Industry-affiliated technologies, including active cyber defense measures to deepen our understanding of threats, enhance the security of UK public and private sector systems and networks facing those threats, and prevent malicious activity; Development and deployment.
* The National Cyber ​​Security Center (NCSC) government has established a single central body for cybersecurity at the national level. The organization will manage national cyber incidents, provide the center of authoritative voice and expertise in cybersecurity, and provide tailored support and advice to departments, delegated administrations, regulators and businesses. NCSC will analyze, detect, and understand cyber threats, and also provide cybersecurity expertise to assist governments in fostering innovation, supporting the thriving cybersecurity industry, and promoting cybersecurity technology development. The only parent for these public institutions is GCHQ, so it can derive world-class expertise and its sensitive capabilities, and improve the support it can provide to the economy and society more broadly. Effective implementation of this cybersecurity advice will remain the responsibility of government departments.

## IMPLEMENTATION PLAN

### 5.1. Defend

The defensive element of this strategy aims to make the UK network, data and systems in the public, commercial and private sectors resilient and protected against cyber attacks. As all crimes cannot be stopped, it will never be possible to stop all cyber attacks. However, with citizens, education providers, academia, businesses and other governments, the UK significantly reduces our exposure to cyber incidents, protects our most valuable assets, and we all operate successfully and thriving in cyberspace. You can build a defense layer that allows you to. Actions to promote cross-country cooperation and good cybersecurity practices also contribute to our collective security.

The government will take steps to ensure that citizens, businesses, public and private sector organizations and institutions have access to the right information to defend themselves. The National Cyber ​​Security Center provides unified advice to the government for threat intelligence and information assurance, ensuring that we provide tailored guidance for cyber defense and respond quickly and effectively to key events in cyberspace. The government will work with industry and international partners to define how cybersecurity looks to the public and private sector, our most important systems and services, and the economy as a whole. We will build security into every new government and critical system. Law enforcement agencies will work closely with industry and national cybersecurity centers to provide dynamic criminal threat intelligence and promote protection security advice and standards to help industry better defend themselves.

#### 5.1.1. ACTIVE CYBER DEFENCE

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**

In carrying out ACD, the government aims to:

• Making the UK network more resilient makes it a much more difficult target for state sponsored actors and cybercriminals.

• Blocks most high- and low-density malware activity on the UK network by blocking malicious program communication between hackers and victims.

• Develop and increase the scope and scale of government capacity to counter serious national sponsorship and cybercrime threats.

• Protects Internet and communication traffic from kidnapping by malicious actors.

• Strengthen UK critical infrastructure and services to citizens against cyber threats.

• Disrupts the business model of all types of attackers, degrading them and reducing the damage they can cause.

**Approach**

In pursuit of these aims, the Government will:

• Working with the industry, especially Communications Service Providers (CSPs), makes it much more difficult to attack UK Internet services and users and greatly reduces the likelihood of an attack that could have a lasting impact on the UK. This includes phishing, blocking malicious domains and IP addresses, and other steps that prevent malicious program attacks. It will also include measures to secure UK telecommunications and Internet routing infrastructure.

• Increasing the size and development of GCHQ, Department of Defense and NCA capabilities, disrupting the most serious cyber threats.

UK including campaigns by sophisticated cybercriminals and hostile foreign actors

• Better protect government systems and networks, help industries build greater security in the CNI supply chain, make the UK's software ecosystem safer, and provide citizens with automated protection for government online services.

Where possible, these initiatives will be provided through partnerships with industry. For many, the industry will design and lead implementation, with professional support, advice, and thought-leadership, along with a significant contribution from the government. In addition, the government will take specific measures to implement these measures, including:

• Block malicious program attacks in cooperation with CSP. We will do this by limiting access to certain domains or websites that are the source of malware. This is called DNS (Domain Name System) blocking/filtering.

• Phishing relying on domain'spoofing' (emails from certain senders, such as banks or government departments, but actually fraudulent e-mails) by deploying e-mail verification systems as standard on government networks and encouraging the industry to do this. Prevent activity.

• Promote security best practices through the multi-stakeholder Internet Governance Organization, such as the Internet Address Management Organization (ICANN), the Internet Engineering Task Force (IETF), and the European Regional Internet Registry (RIPE), which coordinate the domain name system, and the United Nations' stakeholders. Facilitate collaboration with othersTernet Governance Forum (IGF);

• Working with law enforcement channels to protect UK citizens from being targeted for cyber attacks from unprotected offshore infrastructure

• Efforts to implement controls to protect routing

Internet traffic to prevent government departments from being illegally reassembled by malicious actors.

• Invest in the Department of Defense, NCA and GCHQ's programs to improve the ability of these organizations to respond to and disrupt serious national support and criminal cyber activities targeting UK networks.

As the threat evolves, we will develop this technological intervention to ensure that British citizens and businesses are fundamentally protected from the majority of large-scale commodity cyber attacks..

The government measures progress against the following outcomes to determine whether it has succeeded in establishing an effective ACD.

* The UK has large-scale defenses against the use of malicious domains, more aggressive anti-phishing protection at scale, and uses other forms of communication, such as'Vising' and SMS spoofing, to carry out social engineering attacks. It is more difficult to'phish' because things are much more difficult.
* Much more of malware communication and technical facts related to cyber attacks and exploitation are being blocked.
* UK internet and telecommunications traffic is significantly less vulnerable to rerouting by malicious actors.
* Significant improvements in GCHQ, military and NCA capabilities to counter serious national sponsorship and crime threats.

#### 5.1.2. BUILDING A MORE SECURE INTERNET

Technological change gives us the opportunity to significantly reduce the enemy's ability to conduct cybercrime in the UK by ensuring that future online products and services are'basically safe'. This means that the security controls built into the software and hardware we use will be activated with default settings by the manufacturer so that the user can experience the maximum security provided by the user, unless they actively turn off the software and hardware. The challenge is to make transformational changes in ways that support end users and provide commercially viable but secure products or services within the context of maintaining the free and open nature of the Internet.

Governments are leading the way in exploring those new technologies that better protect our own systems, build greater security in the supply chain, secure the software ecosystem, and provide automated protection for citizens accessing government services online. It is in a good position to serve as a phosphorus. Governments must test and implement new technologies that provide automated protection for government online products and services. Where possible, similar skills should be provided to civilians and citizens.

**Objective**

Most online products and services in use are'basically safe' by 2021. Consumers can basically choose products and services with built-in security features. You can turn this off if you want, but consumers who want to join cyberspace in the safest way are automatically protected.

**Approach**

We will pursue the following actions.

* The government will set an example by operating security services on the Internet that do not depend on the security of the Internet itself.
* The government will explore options to work with the industry to develop advanced methods for'basic security' of hardware and software.

We will adopt new cybersecurity technologies that challenge governments, encouraging delegated administrations to reduce the risk of adoption.

This 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. 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.

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.

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.

face of continuous attempts by hostile actors to gain access to government and public sector networks and data.

### 5.2. PROTECTING GOVERNMENT

The UK government, the mandate administration, and the wider public sector have large amounts of sensitive data. They provide essential services to the people and operate networks that are important to national security and resilience. The government's system supports the functioning of our society. The modernization of public sector services will be the cornerstone of the UK's digital strategy, and the government's digital ambitions will make Britain the world's leading digital country. Data held to maintain citizens' trust in online public sector services and systems

It must be protected by the government and all departments of the government must implement an appropriate level of cybersecurity to attack. This ensures accurate and up-to-date knowledge of all systems, data and who can access it. The likelihood and impact of cyber thinking will be minimized by implementing best practices set by NCSC.

The government will also ensure that it can effectively respond to cyber incidents through incident testing and regular testing of government networks. We will invite delegated administrations and local government authorities as necessary to participate in these trainings. With automatic detection, we will be able to better understand the government's online security status.

Cyber ​​security isn't just about technology. Almost every successful cyber attack has a contributing human factor. Therefore, we will continue to invest in our people to ensure that everyone in the government has a sound awareness of cyber risks. We will develop specific cyber expertise in areas where risk is escalating and have the right processes to effectively manage these risks.

NCSC will develop the world's best cybersecurity guidelines to keep pace with new technology threats and development. We will take steps to ensure that government agencies have easy access to threat information to inform their own understanding of cyber risk and take appropriate action.

We will continue to improve our top-class network to protect the government's most sensitive communications.

Health and medical systems pose unique challenges in the context of cybersecurity. The sector employs approximately 1.6 million people in more than 40,000 organizations, and each workforce has significantly different information security resources and capabilities. National Data Guardian for Health and Care has set new data security standards for the UK's health and social care systems, along with a new patient consent/option model. The government will work with health and social services agencies to implement this standard.

"The UK is a global leader in cybersecurity, but as threats are increasing, this new cybersecurity operations center will ensure the safe operation of our troops. The increased defense budget will allow us to stay ahead of hostile forces in cyberspace. He said it means that he can also invest in conventional abilities.

(Rt Hon Michael Fallon MP, Secretary of Defense, April 2016)

Cyber ​​security is essential for our defense. Our military relies on information and communication systems in the UK and around the world. The Department of Defense's infrastructure and manpower are prominent. Defense systems are targeted by criminals, foreign intelligence agencies and other malicious actors who regularly exploit people, disrupt business and operations, and attempt to corrupt and steal information. We will strengthen cyber threat recognition, detection, and response capabilities through the development of the Cyber ​​Security Operations Center (CSOC), which uses the state-of-the-art defense cyber function to protect the Ministry of Defense's cyber space and respond to threats. CSOC will work closely with NCSC to address MoD's cybersecurity challenges and contribute to wider national cybersecurity.

Governments measure progress on the following outcomes to measure success in protecting government networks, systems and data.

• The government has an in-depth understanding of cybersecurity risk levels across government and across the public sector.

• Individual government departments and other agencies protect themselves in proportion to the level of risk and the minimum agreed government standards.

• Government ministries and the broad public sector are flexible and effectively respond to cyber incidents, maintain function and recover quickly.

• Cyber ​​security is basically maintained for new technologies and digital services established by the government.

The cybersecurity of certain UK organizations is particularly important. This is because a successful attack on them will have the greatest impact on UK national security. These impacts can affect the lives of British citizens, the stability and power of the British economy, or the international reputation and reputation of the UK. This group of premium companies and organizations within the public and private sectors includes a critical National Infrastructure (CNI) that provides essential services to the state. Ensuring the safety and resilience of the CNI against cyberattacks will be a government priority. The premium group also includes other companies and organizations that need a higher level of support beyond the CNI. These include:

• The UK's most successful companies and companies that hold our future economic power in the value of research and intellectual property, jewels in our economic crown.

• Data holders – Organizations with large amounts of personal data, as well as organizations with data on vulnerable groups at home and abroad, such as charities.

• Highly threatened – targets such as media organizations that can undermine British reputation, undermine public confidence in government, or jeopardize freedom of expression.

• Touchstone of the digital economy – a digital service provider that enables e-commerce and the digital economy and relies on consumer confidence in services.

• An organization that can leverage the power of the economy as a whole to improve cybersecurity, such as insurers, investors, regulators and expert advisors, through market power and authority.

More action is needed to protect this important part of our economy and support organizations that have a huge impact on others. In both the private and public sectors, our CNI continues to be targeted. Cyber ​​risk across these and many other priority areas is still poorly understood or managed as threats diversify and increase. The UK government will work with Devolved Administrations and other responsible authorities as appropriate to ensure that the UK's most important organizations and businesses, including the CNI, are sufficiently secure and resilient when faced with cyberattacks. Neither the government nor any other public agency will be held responsible for managing these risks for the private sector with boards, owners and operators. However, the government will provide support and guarantees proportional to the threats these companies and organizations face and the consequences of their attacks.

Organizations and corporate boards are responsible for ensuring that their networks are secure. They need to identify critical systems and regularly assess vulnerabilities to evolving technological environments and threats.

Currently, we need to invest in technology and staff to reduce vulnerabilities.

In future systems and supply chains to maintain cybersecurity levels proportional to risk. They should also test their ability to respond in the event of an attack. In the case of the CNI, you can be sure that cyber risks are being managed properly, or else you will need to do this with government agencies and regulators to intervene in the interests of national security.

Therefore, the government will understand the cybersecurity level of our CNI as a whole and will take steps to intervene if necessary to drive improvements that meet national interests.

The government will:

• Share the threat information that only governments can get with the industry so they know what they need to protect.

• Provide advice and guidance on how to manage cyber risk, and work with industry and academia to define cybersecurity excellence.

• Promote the adoption of advanced security needed to protect CNI, such as educational facilities, laboratories, security standards and consulting services.

• Practice practicing cyber risk and vulnerability management with CNI companies.

 NCSC will provide these services for the UK's most important companies.

And organizations including the CNI. It will do so in cooperation with departments and regulatory agencies to ensure that cyber risk is managed in their sectors to the level required by national interests.

The government will also ensure that the right regulatory framework for cybersecurity is in place.

• Ensure industrial activities to protect themselves from threats.

• Focus on results and be flexible enough to stay behind threats or lead to compliance rather than sound risk management.

• Agile enough to promote growth and innovation rather than drive it

• harmonize with the powers of other jurisdictions so that British companies do not suffer from a fragmented and burdensome approach.

• Gives the UK a competitive advantage when combined with effective government support.

Much of our industry is already regulated by cyber security. Nevertheless, we must ensure that corrective measures are taken across the economy, including the CNI, to manage cybersecurity risks.

The government measures progress on the following outcomes to measure success in protecting CNI and other priority areas.

• We understand the level of cybersecurity across the CNI and are taking steps to intervene to improve national interests if necessary.

• The most important companies and organizations understand threat levels and implement proportional cybersecurity practices.

### 5.3. CHANGING PUBLIC AND BUSINESS BEHAVIOURS

A successful UK digital economy relies on corporate and public trust in online services. The UK government has worked with other parts of the industry and the public sector to raise awareness and understanding of the threat. The government also provided public and business access to some of the tools needed to protect themselves. There are many places, world-leading organizations, and organizations that are doing great in providing services to others online, but the vast majority of businesses and individuals still do not adequately manage cyber risk.

“Last year, the average cost of a breach by a large company was £36,600. For a small business, the average breach cost was 3,100 pounds. 65% of large organizations reported having experienced information security breaches over the past year. , 25% of them have experienced at least one violation per month, nearly 7 out of 10 attacks being viruses, spyware, and malicious programs that could have been prevented using the government's cyber essentials." (2016 Government Cyber ​​health checkup and cyber security breach investigation)

**Objective**

The goal is to ensure that individuals and organizations of all sizes and sectors take appropriate steps to protect themselves and their customers from cyber attacks.

**Approach**

The government will provide advice that the economy needs to protect itself. We will improve how this advice is delivered to maximize its effectiveness. For the public, the government will use'trusted voices' to increase the scope, reliability and validity of our messages. We will provide easy-to-action, personally relevant advice when they access the service and are at risk. We will engage delegated administrations and other authorities at the right time.

For companies, we will try to help companies leverage cyber risk management through organizations such as insurance companies, regulators and investors. This will highlight the price of cyber risks caused by clear business interests and market influencers. We will better understand why many organizations still do not adequately protect themselves, and work with organizations like professional standards bodies to persuade companies to take action beyond raising awareness. We will also ensure that we have the right regulatory framework to manage cyber risks that the market cannot address. As part of that, we will seek to raise the standard of cyber security and protect citizens using levers like the GDPR.

UK individuals, organizations and organizations have access to the information, education and tools they need to protect themselves. In order for us to deliver a step-by-step change in public behaviour, we will maintain a consistent and consistent set of messages on cybersecurity guidelines for both government and our partners. NCSC will provide technical advice to support this guidance. It reflects business and public priorities and practices, and will be clear, easily accessible and consistent, keeping pace with threats. Law enforcement agencies will work closely with industry and NCSC to share the latest criminal threat information, support industries to defend themselves from threats, and mitigate the impact of attacks on British victims.

The government measures progress on the following outcomes to measure success in protecting CNI and other priority areas.

• The UK economy has a cybersecurity level of comparable or higher than that of developed countries.

• The number, severity, and impact of cyber attacks on businesses in the UK has decreased due to improved cyber hygiene standards.

• The cybersecurity culture is improving across the UK, as organizations and the public understand their cyber risk levels and the cyber hygiene steps they need to take to manage them.

### 5.4. MANAGING INCIDENTS AND UNDERSTANDING THE THREAT

The number and severity of cyber incidents affecting organizations across the public and private sectors is likely to increase. Therefore, we need to define how the private sector and the public cooperate with the government during cyber incidents. We will ensure that the level of support in each sector, taking into account the UK government's cyber maturity, is clearly defined and understood. Government information gathering and distribution of threats must be delivered quickly in a way that is appropriate for all types of organizations. The private, government and public sectors currently have access to multiple sources of information, guidance and support for cybersecurity. This should be simplified.

We must ensure that government provision is not isolated, but in partnership with the private sector in responding to incidents and providing guidance. Our incident management process should reflect the holistic approach to incidents by learning from partners and sharing mitigation techniques. We will also continue to use our relationship with other computer emergency response teams (CERTs) and allies as an integrated part of our incident management function.

Current accident management is somewhat shattered across government departments, and this strategy will create a unified approach. NCSC will provide efficient and effective government-led incident response. In the event of a serious cyber incident, we will ensure that the armed forces can assist, whether in the conventional form of dealing with the physical impact, or in the form of expert assistance from regular or prospective cyber agents. While we will provide all the support our resources will allow, the government continues to emphasize the importance of industrial, social and public action to ensure basic cyber security.

**Objectives**

Our goals are:

• The government will provide us with an integrated approach to incident management, based on improved understanding and awareness of the threats and actions against us. NCSC will be a key support organization, as well as partnerships with the private sector, law enforcement agencies and other government departments, authorities and institutions.

• NCSC defines a clear process for incident reporting and adapts it to the victim's profile.

• We will have an effective information sharing structure to prevent the most common cyber incidents and inform our'precautionary' plans.

**Approach**

Public and private sector organizations and corporate executives are responsible for ensuring that the network is secure and implementing an incident response plan. In the event of a serious event, the government's accident management process will reflect three distinct elements of cyber thinking: the global cause, the event itself, and the post-event response. In order to deliver effective accident management to both the government and the private sector, we will carefully examine and define the scope of government response to strengthen cooperation. We will develop a national cyber practice plan by improving our understanding and awareness of threats to improve the provision of support to public and private sector partners.

We will create a trustworthy and reliable government identity for case consultation, support and assurance. This will increase cybersecurity awareness across the UK digital community and enable us to identify trends, take proactive action, and ultimately prevent accidents.

As we move to automated information sharing (ie cybersecurity systems automatically warn each other about incidents or attacks), we will provide more effective services. This will enable organizations to act quickly on relevant threat information.

The government measures the success of the following results to measure the success of incident management.

• A higher percentage of incidents are reported to the authorities to better understand the size and magnitude of the threat.

• Cyber ​​Incident Management NCSC was created as a centralized incident reporting and response mechanism, resulting in more effective, efficient, comprehensive, and

• At the national level, the root cause of the attack will be addressed to reduce the occurrence of repeated exploitation across multiple victims and sectors.

## 6. DEVELOP

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. 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.

### 6.1. STRENGTHENING CYBER SECURITY SKILLS

The UK is a systemic issue at the core of cyber technology shortages: the lack of young people entering the profession, the current shortage of cybersecurity experts, insufficient exposure to cyber and information security concepts in the computer process, and the availability of appropriately qualified teachers. You have to cope with the lack of, and the absence of, established c. Enter the job through land and training.

This calls for rapid government intervention to address current shortage issues and develop a coherent long-term strategy that can bridge the technology gap based on these interventions. However, in order to have a profound impact, it must be recognized that these efforts must cooperate with inputs from influencers and participants across delegated administrations, public sector, education providers, academic institutions and industries.

**Objective**

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.

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.

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.

**Approach**

Based on existing work, we develop and implement an independent technology strategy that incorporates cyber security into the education system. This will improve the overall state of computer science education and include cybersecurity in the curriculum. Everyone who studies computer science, technology, or digital technology will learn the basics of cybersecurity and will be able to incorporate those skills into the workforce. As part of this effort, we will address gender imbalances in cyber-focused jobs, reach out to people from more diverse backgrounds and make sure we are drawing from the widest pool of talent available. We will work closely with the delegated administration to promote consistent access across the UK.

We will more clearly present the roles of government and industry, including how they will evolve over time. The UK government and the mandate administration play a key role in creating the right environment for cybersecurity technology to be developed and updating the education system to reflect the changing needs of industry and government. However, employers also have an important responsibility not only to articulate their needs, but also to train and develop employees and young people entering the profession. Industry plays an important role in establishing diverse and attractive career and training paths in partnership with academics, professional organizations and trade associations.

Recognizing the collective challenges we face in the process of bridging the technology gap, we strengthen the consistency between these core areas by establishing technical advisory groups of governments, employers, professional organizations, technical institutions, education providers, and academia. This subclass will support the development of long-term strategies that consider the development of a wide range of digital technologies while ensuring that cybersecurity considerations are coordinated and integrated as a whole. The group will work with similar groups across the UK.

Along with this work, the government will invest in a variety of initiatives to bring immediate improvement and inform the development of long-term technology strategies. These include:

• Establish school programs to create step-by-step changes in professional cybersecurity education and training for 14-18 year olds (class-based activities, after-school sessions with professional mentors, challenge projects and summer schools)

• Cultivate higher levels of apprentices within the energy, financial and transportation sectors to bridge the technology gap in essential areas.

• Funding to retrain applicants already at work with high potential for cybersecurity professionals

• Acknowledging and supporting educational post-graduate and post-graduate education, identifying and closing professional skills gaps, and acknowledging the key role universities play in technology development

• Support teacher professional development certification in cyber security. This will help teachers and other learners understand cybersecurity education and provide these individuals with a way to authenticate externally.

* Focus on cybersecurity expertise by 2020, earning the status of Royal Charterd, strengthening organizations recognized for excellence in cybersecurity in the industry, and providing a focal point to advise, shape and promote national policies. Develop Defense Cyber ​​Academy as a center of excellence in cyber training, training to deal with professional skills and broad education across the Department of Defense and a wide range of governments.

Develop facilities to maintain and practice opportunities and skills to collaborate in training and education between government, armed forces, industry and academia.

* • We will work with the industry to expand the CyberFirst program to identify and foster a diverse pool of young talent to protect national security.
* • Embed cybersecurity and digital technology as an integral part of the relevant process within the education system, from elementary to graduate school, setting standards, providing quality and a solid foundation for future field progress. Education is a mandated issue, so some of these initiatives will mainly apply in the UK. However, we will collaborate with a mandated administration to promote a consistent approach across the UK education system.

The government measures our success in strengthening cybersecurity technology by evaluating progress on the following outcomes:

* There is an effective and clear path to cybersecurity and is attractive to a wide variety of people.
* By 2021, cybersecurity is effectively learned as an essential part of the relevant process, from the primary to the post-stage.
* Cybersecurity is widely regarded as an established career with a clear path and has earned the Royal Chartered status.
* Proper cybersecurity knowledge is an essential part of continuing professional development for relevant non-cybersecurity professionals across the economy. And government, military and military can take advantage of cyber experts who can maintain UK security and resilience.

### 6.2. STIMULATING GROWTH IN THE CYBER SECURITY SECTOR

The fast-growing and innovative cybersecurity sector is a necessity of the modern digital economy. UK cybersecurity companies provide the world's best technology, training and advice to industry and government. But while the UK is a leader, it faces fierce competition to stay ahead. There are also barriers that the government must address. British entrepreneurs and scholars develop advanced technology, but some need support to develop the commercial and entrepreneurial skills needed to thrive. There are funding gaps that prevent SMEs from growing and expanding into new markets and territories. The most breakthrough products and services that offer us the potential to stay ahead of the threat are trying to find customers who are willing to act as early adopters. To overcome these challenges, government, industry, and academia must cooperate effectively.

**Objective**

The government will support the creation of a growing, innovative and thriving cybersecurity sector in the UK to create the following environment:

* Security companies thrive and receive the investment they need to grow.
* Top talents from government, academia and the private sector work closely together to promote innovation.
* Government and industry customers are well prepared to adopt the latest services.

**Approach**

To build this ecosystem, do the following:

• Commercialize academic innovation and provide training and mentoring to academics.

• Establish two innovation centers to promote the development of advanced cyber products and dynamic new cyber security companies. This innovation center is at the heart of the initiative's program to provide startups with the support they need to win their first customers and attract additional investments.

• Allocating a £157 million Defense and Cyber ​​Innovation Fund ratio to support innovative procurement in defense and security.

• Provide test facilities for companies to develop products, and quickly provide evaluation methods that customers can use with confidence as next-generation cyber security products and services emerge.

• Leverage the collective expertise of the industry-government cyber growth partnership to shape and focus further growth and innovation interventions.

• Support scale-up and international market access for companies of all sizes

• Promote agreed international standards that support access to the UK market.

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.

**Measuring success**

The government measures progress on the following outcomes to determine whether it has succeeded in driving growth in cybersecurity.

* UK's annual cyber sector growth above average worldwide
* Significant increase in investment in early stage companies
* Adoption of more innovative and effective cybersecurity technologies to the government.

Commercially successful products and services The UK will maintain a reputation for innovative excellence, including areas of exceptional national power, such as the financial sector draw close To achieve this, the government will encourage collaboration for research, innovative and flexible funding models, and commercialization of research. The government will pay full attention to the human and behavioral aspects of cyber, and ensure that systems beyond technical scope such as business processes and organizational structures are included in cyber science and technology. This will support the creation of products, systems and services that take into account proper security from the start and become'basically secure' where security becomes a conscious'option out' to the user.

After thorough consultation with partners and stakeholders, we will announce a specific cyber science and technology strategy. This will include identifying areas of science and technology that governments, industries and academia deems important and identifying gaps in the UK's current capacity to address them.

The government will continue to fund and support academic centers, research institutes, and doctoral education centers. We will also create a new research institute for strategically important subject areas. We will also sponsor further research in areas where the upcoming cyber science and technology strategy identifies gaps in capabilities. Important areas to come Big data analysis, autonomous systems, and reliable systems are considered..

### 6.3. PROMOTING CYBER SECURITY SCIENCE AND TECHNOLOGY

Britain's thriving science and technology sector and state-of-the-art research support our world's best cybersecurity capabilities. In order to maintain and enhance the UK's reputation as a global leader in advanced research, our academic research institutions need to continually attract the best and smartest in cybersecurity. To this end, it is necessary to cultivate excellent centers that attract the most competent and dynamic scientists and researchers, and deepen the active cooperation between academia, government, and industry. This will include a matchmaking role for governments that encourage us to cooperate. Success will see us establishing a self-sustaining ecosystem that allows ideas and people to cycle between the three areas in a mutually beneficial way.

**Objective**

By 2021, the UK will strengthen its position as a world leader in cyber science and technology. Flexible partnerships between universities and industries will transform research into industrial control systems, cyberphysical systems and the Internet of Things, smart cities, automated system verification, and cybersecurity science.

We will continue to increase the number of UK nationals with cyber expertise by sponsoring UK PhD students at the Academic Centers of Excellence.

The government will cooperate with institutions including the UK of Innovation and Research Council to encourage cooperation between industry, government and academia. To support this collaboration, we will review best practices for security classification and identify security deletion experts, including academics. This will ensure that the work from unclassified space to beyond the secret can be as cooperative as possible.

The government will fund some of the most pressing issues in cybersecurity and fund the "Great Challenge" to provide innovative solutions. CyberInvestment, a new industrial and government partnership to support advanced cybersecurity research and protect the UK in cyberspace, will be part of our approach to building academic-government-industry partnerships.

**Measuring success**

The government measures the progress of cybersecurity science and technology promotion by evaluating progress against the following results.

* • The number of UK companies that have successfully commercialized academic cyber research has increased significantly, and effective measures to close them have narrowed the consensus and identified gaps in UK cybersecurity research capabilities.
* • The UK is considered a global leader in cybersecurity research and innovation.

### 6.4. EFFECTIVE HORIZON SCANNING

Governments should ensure that policymaking takes account of changing cyber, geopolitical and technological landscapes. This requires effective use of wide horizon scanning and evaluation. We need to invest in preparing for future threats and anticipate market changes that could affect our cyber resilience in 5 to 10 years. We need a horizontal scanning program that generates recommendations to inform current and future government policies and program plans.

**Objective**

The government will ensure that our Horizon Scanning Program includes a rigorous assessment of cyber risks, which will be integrated into cyber security and other technical policy development areas, and all source assessments and other available evidence. We will participate in the horizon search between national security and other policy areas to ensure a holistic assessment of new challenges and opportunities.

**Approach**

The government will:

* Coordinate work across discipline boundaries to identify current business differences and develop a holistic approach to horizontal search for cybersecurity.
* Promote better integration of technical aspects of cybersecurity and behavioral science.
* Support rigorous monitoring of the cybercrime market to discover new tools and services that enable technology transfer to hostile countries, terrorists or criminals.
* Analyze new Internet connection process control techniques.
* Prediction of vulnerability around digital currencies
* Monitor market trends in communications technology to develop early defense against anticipated future attacks.

We recognize that horizon scanning goes beyond technical to include political, economic, legislative, social and environmental dimensions. Cyber security is only one aspect of the problem that effective horizon search can solve. Therefore, we will ensure that any impact on cybersecurity is taken into account when conducting horizontal searches for these other policy areas.

We will also ensure that cyber policymaking follows an evidence-based approach, taking into account the assessment of all possible sources. This includes, for example, the future role of certain technical evidence or advanced materials on the Internet of Things. International strategic and societal trends and their impact on cyber.

We consider cybersecurity within the authority of the Intergovernmental Emerging Technology and Innovation Analysis Cell (ETIAC) to be established to identify technology threats and opportunities related to national security, and cybersecurity in existing horizontal scanning structures, including government F. Consider using the Group (GFG) and the Cabinet Minister Advisory Group (CSAG).

**Measuring success**

The government will measure our success in establishing effective horizontal inspection capabilities by evaluating progress toward outcomes such as:

* Intergovernmental horizon scanning and all source assessments are integrated into cyber policy making.
* The impact of cybersecurity is reflected in all intergovernmental horizon searches.