HM Government

National Cyber Strategy 2022

Pioneering a cyber future with the whole of the UK

National Cyber Strategy 2022

Pioneering a cyber future with the whole of the UK

목차

추가 목차

서문

영국은 협력과 혁신의 결과로 외부지향적 세계 국가의 성공을 거둔 개방적이고 민주적인 사회이다. 이 사실은 국제 보건 비상사태에 대한 대응과 Net Zero (탄소 중립) 목표 활동에 잘 나타나 있다. 이러한 협력과 혁신의 결과가 가장 도드라지게 나타나는 분야가 사이버 분야이다.

사이버가 국민과 경제에 제공하는 넓은 범위의 이익은 우리가 국가로서 한 단계 성장시키고 통합시키는 것이든, 국가 가치관을 반영하는 사이버 공간에 관하여 파트너들과 협력하고, 국제적인 사건들에 사이버 능력의 영향력을 행사하는 것이든, 영국은 사이버를 기술의 발전으로 인해 변화하는 세상에서 국익을 보호하고 증진 시키는 방법으로 봅니다.

새로운 국가 사이버 전략은 영국이 빠르게 변화하는 디지털 세계에서 자신감, 역량 및 회복력을 유지할 수 있도록 보장하기 위한 계획이며, 사이버 공간에서 우리의 이익을 보호하고 증진시키기 위해 적응하고, 혁신하며, 투자하고자 하는 계획을 담고 있다.

2016년의 선구적인 국가 사이버 안보 전략에 이어, 이번 국가 사이버 전략으로 더욱 탄력적으로 대응 할 수 있는 미래로 우리를 이끌고자 한다. 담당 수석 장관으로서, 나는 두 가지 핵심 목표를 명백히 하고자 한다. 첫째, 사이버의 핵심 기술을 강화해야 한다는 것; 둘째, 우리와 가치관을 공유하지 않은 체제 하에서 개발된 개별 공급자나 기술에 대한 의존도를 줄여야 한다는 것이다.

영국의 과학과 기술은 이 변화의 동력이 될 것이며, 사이버 기술이 국가 경제적 및 전략적 자산이 되고, 우리의 기술이 보다 신뢰할 수 있으며, 최근까지도 그 역량이 국가의 전유물이었던 다층의 사이버 적대자들을 더 잘 막아낼 수 있도록 할 것이다.

정부 차원에서 우리는 연구 개발에 220억 파운드를 투자하고 국가 안보 계획의 중심에 기술을 둘 것이다. 우리 모두는 디지털 기술의 변화 가능성도 보았고, 5G와 같이 기술이 가져올 수 있는 혼란도 경험했다. 우리의 인공지능 및 데이터 정책 계획은 우리가 이러한 기술에 선두에 설 수 있도록 할 것이며, 사이버 전략 하에서 취한 조치들이 우리가 공급자와 파트너의 보안과 회복력에 대한 확신을 가질 수 있도록 할 것이다.

작년 국가 사이버 부대 창설은 우리의 사이버 공격 능력의 중요한 발전을 의미한다. 그러나 기본적인 사이버 보안의 핵심은 영국과 우리 시민들을 공격하는 사람들에 대한 대응을 강화함에 있다. 또한 공공 기관을 보다 회복력 있게 만들어 의회가 랜섬웨어 및 기타 사이버 공격으로부터 시스템과 시민의 개인 데이터를 보호할 수 있도록 지원하는데 초점을 맞추고 있다.

사회 차원에서 사이버는 모두를 위한 것입니다. 이 전략을 바탕으로, 정부는 영국 시민들과 기업들, 그리고 국제적 협력 파트너들을 보호하기 위해 더 많은 노력을 하고 있다. 영국은 사이버 공간의 미래가 모든 사람들과 기업이 번창하는 신뢰적이고 탄력적인 공간이라는 것을 믿을 수 있게 최선을 다 할 것이다.

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

개요

디지털 시대의 기회와 과제

1. 기하급수적인 기술의 발전과 비용 절감으로 인해 세계는 그 어느 때보다 더 연결되었고, 이는 엄청난 기회와 혁신과 발전을 이끌고 있다. 코로나 바이러스 (COVID-19) 펜데믹은 이러한 추세를 촉진하였고, 우리는 여전히 장기적인 구조적 변화의 초기 단계에 있는 것 같다. 사이버 공간의 세계적인 확장은 우리가 살고, 일하고, 소통하는 방식을 바꾸고 있으며, 우리가 의존하는 중요한 시스템인 금융, 에너지, 음식 유통, 의료, 교통과 같은 분야를 변화시키고 있다. 간단히 말해서, 사이버 공간은 현재 우리의 미래 안보와 번영에 필수적인 공간이다. 사이버 공간은 영국과 같은 기술적으로 선진화된 국가가 새로운 방식으로 그들의 국가 목표를 추구할 수 있는 특별한 기회를 제공한다.

2. 이러한 변화의 규모와 속도는 때로는 사회 규범, 법률 및 민주주의 제도를 뛰어넘고, 또한 한편으로는 전례없는 복잡성, 불안정성 및 위험을 야기하고 있다. 지난 해에는 병원과 송유관, 학교와 기업에 대한 사이버 공격이 있었으며 일부는 랜섬웨어와 활동가, 언론인, 정치인을 대상으로 한 상업용 스파이웨어로 인해 중단되었다. 사이버 공간의 초국가적 성격은 국제적인 협력 없이는 이러한 어려움을 해결할 수 없다는 것을 의미하고, 또한 사이버 공간은 중요한 시스템 경쟁의 장이자 우리의 글로벌 미래의 이익, 가치 및 비전의 경쟁이 충돌하는 공간이기도 하다.

우리의 비전: 국가적 목표를 성취하기 위한 사이버 파워

3. 이런 관점에서 사이버 전력은 국력과 전략적 이점의 근원으로서 어느 때 보다 더 중요한 도구가 되어 가고 있다. **사이버 전력은 사이버 공간에서 그리고 사이버 공간을 통해 국익을 보호하고 증진시키는 능력이다.** 디지털 시대의 기회와 과제를 가장 잘 헤쳐 나갈 수 있는 국가가 미래에 더 안전하고 회복력 있으며 번영할 것이다. 영국은 세계에서 가장 디지털화된 선진국 중 하나이며 영국 정부는 국내외적으로 야심 찬 테크놀로지 아젠다를 가지고 있다. 이 사실은 우리가 특히 사이버 공간의 도전에 노출되어 있다는 것을 의미하지만, 다른 한편으로는 우리의 국민과 인류 공동의 이익을 추구하는 기회를 취함에 있어 선도할 수 있는 특별하게 잘 준비되어 있음을 의미한다.

4. 향후 10년 동안 인터넷, 디지털 기술 및 이를 뒷받침하는 기반 시설은 우리 영국, 동맹국 및 적대국의 이익에 핵심이 될 것이다. 경쟁이 심화되어 있는 시대에 사이버 전력을 강화함으로써 영국의 새로운 역할을 구축하여, 기업과 다른 국가들을 선도하고, 미래 기술 변화에 앞서 나아가고, 위협을 완화하고, 적과 경쟁자들로부터 전략적 우위를 점하게 될 것이다. 그리하여 영국을 거주하며, 기업 활동을 하고, 투자하기에 가장 안전하고 매력적인 디지털 경제로 만들 것이다.

5. 우리의 비전은 **2030년에도 영국이 계속해서 국가 목표를 위해 책임감 있고 민주적인 사이버 파워 주도국으로서 사이버 공간에서 그리고 사이버 공간을 통해 우리의 이익을 보호하고 증진 시키고자 하는 것이다.** 즉,

- 진화하는 위협과 위험에 더 잘 대비하고, 범죄, 사기 및 국가 위협으로 부터 시민을 보호하기 위해 우리의 사이버 능력을 활용하여 보다 안전하고 회복력 있는 국가
- 국가 전체와 다양한 사람들에게 고르게 분배하는 기회를 제공하는 혁신적이고 번영하는 디지털 경제
- 보다 친환경적이고 건강한 사회를 지향하며 혁신 기술을 활용하는 과학과 기술의 초강대국
- 사이버 공간에서 행동의 자유를 유지하며, 개방적이고 안정적인 국제 질서의 미래 경계를 형성하고, 국제적으로 더 영향력 있고 가치 있는 파트너

6. 지난 10년 동안 우리 영국은 첨단 사이버 보안 및 운영 능력을 개발하여 사이버 보안 분야에서 주도적 사이버 강국으로서 자리매김을 하였다. 이 전략은 2016-2021 국가 사이버 보안 전략을 바탕으로 이루어진 중요한 진전과 정부의 보안, 국방, 개발 및 외교 정책에 대한 통합 검토서(Integrated Review)에서 제시된 세 가지 중요한 결론을 기반으로 한다. 첫째, 디지털 시대에 영국의 사이버 파워는 우리의 국가적 목표를 달성하는 데 있어 그 어느 때보다 중요한 요소가 될 것이다. 둘째, 우리의 사이버 파워를 유지하기 위해서는 우리의 사이버에서의 목표와 능력을 모두 고려하여 보다 포괄적이고 통합된 전략이 필요하다. 셋째, 이 전략은 전 사회적 접근법으로 이루어져야 한다 – 기업이나 학교에서 일어나는 일은 기술 전문가와 정부 관계자들의 행동만큼이나 국가 사이버 파워에 중요하며, 협력 관계를 통해 노력하는 것이 우리의 성공에 필수적일 것이다.


CHELTENHAM
Science
Festival
18.2 Cyber Skills

사이버 전략의 5대 전략 축

7. '통합 검토서'(IR)에서는 이 전략에 대한 5가지 '우선 실행 계획'을 제시했으며, 이 다섯 가지 전략 축은 **2025년까지 달성하고자 하는 목표와 우리가 취하려는 구체적인 실행 계획을 정립하기 위한 전략적 기반으로 사용할 것이다.**

- **전략 축 1: 영국의 사이버 생태계 강화,** 정부, 학계, 산업계의 협력을 심화하고 인력과 기술에 투자한다.
- **전략 축2: 회복력 있고 번영하는 디지털 영국 구축,** 기업이 디지털 기술의 경제적 이점을 극대화할 수 있도록 사이버 위험을 줄이고, 국민들이 온라인에서 보다 안전하고 데이터가 보호된다는 확신을 갖게 한다.
- **전략 축3: 사이버 파워에 필수적인 기술 선도,** 우리의 산업 역량을 구축하고 미래 기술을 확보하기 위한 틀을 개발한다.
- **전략 축4: 보다 안전하고 번영하며 개방적인 국제 질서를 위한 영국의 글로벌 리더십과 영향력 향상,** 정부 및 산업 파트너와 협력하고 영국의 사이버 파워를 뒷받침하는 전문성을 공유한다.
- **전략 축5: 우리의 위협이 되는 적들을 탐지, 방해 및 저지함으로써 사이버 공간에서의 영국 안보 강화,** 영국의 모든 범위의 영향력을 보다 통합적이고 창의적이며 일상적으로 사용하도록 한다.

8. 이 문서의 1장에서는 우리가 운영하고 있는 전략적 맥락, 전략의 목표, 그리고 향후 10년 동안 전략적 접근에 대해 설명한다. 2장에서는 2025년 우리의 목표를 달성하기 위해 이 다섯 가지 전략 축 아래에 우리가 취할 구체적인 실행 계획을 설명한다.

비전

영국은 2030년까지 책임감 있고 민주적인 사이버 강국으로써 국가 목표를 위해 사이버 공간에서 그리고 사이버 공간을 통해 우리의 이익을 보호하고 증진시킬 수 있게 할 것이다.

전략 축과 목표

전략 축 1

영국의 사이버 생태계 강화

1. 사이버에 대한 전 사회적 접근을 위해 필요한 체계, 파트너십 및 네트워크를 강화한다.
2. 차세대 재원들이 관심을 가질 수 있는 다양하고 세계적인 수준의 사이버 전문직을 포함한 모든 분야에서 국가 사이버 능력을 높이고 확대한다.
3. 지속 가능하며, 획기적이며, 국제적으로 경쟁력이 있는 사이버 및 정보 보안 분야의 성장을 촉진하여 정부와 경제 전반의 요구를 충족하는 양질의 제품과 서비스를 제공한다.

전략 축 2

회복력 있고 번영하는 디지털 영국 구축

1. 사이버 보안 및 복원력에 대한 보다 효과적인 조치를 취하기 위해 사이버 리스크에 대한 이해를 높인다.
2. 사이버 공격을 예방하고 맞서기 위해 영국 기관 내의 사이버 리스크 관리를 개선하여 국민을 보호한다.
3. 사이버 공격에 대비, 대응 및 복구하기 위해 국가 및 관리 기관 차원의 복원력을 강화한다.

전략 축3

사이버 파워에 필수적인 기술 선도

1. 사이버 전력에 가장 중요한 과학 기술 개발을 예측, 평가 및 수행할 수 있는 능력을 개선한다.
2. 사이버 공간에 중요한 기술의 보안에서 독립적 그리고 협력적 이점을 강화하고 유지한다.
2a. 범 정부 고객, 파트너 및 동맹의 요구사항을 충족하고 가장 유능한 적들의 위협을 포함하여 가장 큰 위험을 적절히 완화하는 강력하고 탄력적인 국가 암호 키 기업을 지원한다.
3. 차세대의 연결 기술 및 인프라를 확보하여 글로벌 시장 의존에 의한 사이버 보안 위험을 완화하고 영국 사용자가 신뢰할 수 있고 다양한 공급이 가능하게 한다.
4. 우리의 민주적 가치를 지키고, 사이버 보안 확보 및 과학기술을 통한 영국의 전략적 우위 증진을 위해, 다중 투자자 커뮤니티와 협력 하에 가장 중요한 우선순위 영역에서 글로벌 디지털 기술 기준의 개발한다.

전략 축4

영국의 글로벌 리더십과 영향력 향상

1. 국제 파트너의 사이버 보안 및 복원력을 강화하고 적의 방해 및 저지하기 위해 공동의 조치를 취해야 한다.
2. 자유롭고 개방적이며 평화롭고 안전한 사이버 공간을 위해 글로벌 거버넌스를 구축한다.
3. 영국의 전략적 이점을 강화하고 보다 광범위한 외교 정책 및 번영 이익을 증진시키기 위해 영국의 사이버 능력과 전문 지식을 활용한다.

전략 축5

우리의 위협되는 적들을 탐지, 방해 및 저지

1. 범죄 및 기타 악의적인 사이버 활동에 대한 정보를 공유하고 탐지, 조사함으로 영국과 영국의 이익 및 국민을 보호한다.
2. 영국, 영국의 이익 및 시민에 반하는 국가, 범죄자 및 기타 악의적인 사이버 활동가 및 그들의 활동을 저지하고 파괴한다.
3. 우리의 국가 안보와 중대 범죄의 예방과 탐지를 지원하기 위해 사이버 공간 안팎에서 조치를 취한다.

추가적 국가 목표

- **보안과 복원력**
- **과학기술 초강대국**
- **경제 번영**
- **국제 질서 수립**

Part 1:
전략

전략적 맥락

경쟁 시대의 글로벌 영국

9. 2021년 3월 발표된 안보·국방·개발·외교정책 '통합 검토서'(IR)는 향후 10년간 세계에서 영국의 역할에 대한 정부의 비전과 우리가 2025년까지 취할 실행 계획을 설명하고 있다. 영국이 보다 경쟁력 있는 세계에 더 잘 대비하기 위해서는 우리의 국가적 번영과 전략적 이점을 증진시키기 위한 과학 기술의 혁신을 수용해야 한다는 것을 인식하고 있다. 국가 사이버 전략은 이러한 접근 방식을 기반으로 하며 그 출간으로 '과학 및 기술을 통한 전략적 이점 유지'라는 통합 검토서의 전략 목표에 따른 공약의 일부를 발표하는 것이다.

사이버 환경

10. 사이버 공간이 제시하는 정책적 난제는 본질적으로 기술적 문제만은 아니다. 사이버 영역은 인간이 만든 환경이며 인간의 행동 양식에 의해 기본적으로 형성된다. 사이버 영역은 좋게든 나쁘게든 그러한 습성을 증폭시키며, 그 영향은 보통 현실 세계에서도 반영된다. 사이버 공간은 민간 기업, 정부, 비영리 단체, 국민 개인, 심지어 범죄자들에 의해 소유되고 운영된다. 즉, 사이버 영역에 대한 전략적 대응은 전략 지정학과 국가 안보, 응용 범죄학과 시민 규제, 경제 산업 정책과 연계되어야 하며 온라인에서 상호 작용하는 다양한 문화적 또는 사회적 상황과 가치 체계에 대한 깊은 이해가 필요하다.

11. 또한 사이버 공간은 국경을 초월한다. 기술 공급망과 의존성은 점점 더 세계화되고, 사이버 범죄자와 국가 지원 활동가들은 전 세계에서 활동하며, 강력한 기술 회사들은 제품을 수출하고 그들의 기준을 설정하며, 사이버 공간과 인터넷을 좌우하는 규칙과 규범들은 국제 무대에서 결정된다. 사이버 공간은 기술과 사람들이 사이버 공간을 이용하는 방식에 따라 지속적으로 진화하며, 우리에게 민첩하고 대응력 있는 접근을 채택할 것을 요구한다.

사이버 공간의 층위

사이버 공간이란?

우리에게 사이버 공간은 소통하고, 일하고, 일상적인 업무를 온라인으로 수행할 때 경험하는 가상 세계이다. 기술 용어로써 사이버 공간은 인터넷, 통신망, 컴퓨터 시스템 및 인터넷 연결 장치를 포함하는 정보 통신 기술의 상호 의존적인 네트워크이다. 군사적으로 사이버 공간에서 위협에 대응하기 위해 노력하는 상태에서는, 육, 해, 공, 우주가 작전 영역이듯, 사이버 공간에서의 위협에 대응하기 위한 작전 영역이다.

우리는 사이버 공간을 어떻게 경험하는가? 사이버 공간은 정의적으로 '공유'된 공간이며, 그 규모와 복합성으로 인하여 모든 사람의 경험이 특별하다는 것을 의미한다. 시민은 온라인으로 은행 계좌를 확인하거나 집에서 영화를 스트리밍할 때 사이버 공간에 접속한다. 기업은 사이버 공간을 활용하여 직원들과 연결하여 필요한 정보를 확보하거나 제조 과정을 통제한다. 정부는 온라인 포털을 이용하여 시민들에게 공공 서비스를 제공한다. 사이버 전문가들은 사용자들에게 '작동' 가능하게 하는 기술, 기준 및 프로토콜을 '심도 있게' 들여다 본다. 이와 같은 각기 다른 그룹은 사이버 공간을 각자 다른 방법과 다른 목적으로 사용하고 있고, 우리는 그 어느 때 보다도 더 많이 사이버 공간을 이용하고 있다.

온라인 체험

- 이메일 계정
- 게임 프로필
- 소셜 미디어 계정
- 은행 계좌 접속
- 비접촉식 승차권
- 운동 추적 프로필

소프트웨어, 시스템, 정보

- 기업 IT 시스템
- 데이터 베이스, 예: 영국 국세청의 납세 기록
- 산업 통제 시스템
- 윈도우/OS
- 어플, 예: WhatsApp, Facebook, TikTok
- 프로그래밍 언어, Python, C++

기기, 통신 수단·라우터, 허브

- 서버
- 와이파이, 이더넷
- 라디오 안테나
- 스마트 냉장고
- 비접촉 여행 카드 리더기
- 핸드폰, 컴퓨터외 개인 기기들

사이버 공간은 세 개의 층위로 설명될 수 있다:

가상 층위

대부분의 사람들이 경험하는 사이버 공간의 형태이다. 가상 층위는 공유된 가상 공간에서 가상 신분을 통한 사람과 기관의 대표성으로 이루어져 있다. 가상 대표성은 이메일 주소, 사용자 ID, 소셜 미디어 계정 또는 가명(닉네임)이 될 수 있다. 온라인에서는 개인이 또는 한 조직이 온라인에서 여러 개의 신원을 가질 수 있고, 반대로, 여러 사람 이나 조직이 하나의 공유된 신원을 생성할 수 있다.

논리 층위

운영 체제, 프로토콜, 응용 프로그램 및 기타 소프트웨어 같이 코드와 데이터로 이루어져있는 부분이다. 논리 층위는 물리적인 층위과 유선 네트워크 또는 전자기적 스펙트럼에서의 정보 흐름 없이는 작동하지 못한다. 물리적 층위와 함께 논리적 층위는 가상 신원이 통신하고 작동할 수 있도록 한다.

물리적 층위

사이버 공간의 물리적 층위는 작게는 가정에 있는 라우터, 전선, 허브에서부터 크게는 일류 첨단 기술 회사가 운영하는 크고 복잡한 통신 시스템까지 데이터가 전송되는 모든 하드웨어를 포함한다. 사이버 공간의 물리적인 층위는 물리적 시설뿐만 아니라 와이파이나 라디오와 같은 데이터가 전송되는 전자기적 스펙트럼도 포함한다.

사이버 전력

12. 우리 전략은 사이버 공간 안과 사이버 공간을 통해 자국의 이익을 보호하고 증진시키는 국가의 능력으로 정의하는 사이버 전력의 개념을 핵심으로 한다. 우리는 사이버 파워의 5가지 광의의 차원을 파악하였고 이들은 이 전략의 핵심 전략 축과 궤를 같이 한다.

- 사이버 파워의 토대가 되는 인력, 지식, 기술, 구조 및 파트너십과 같이 다른 모든 구성 요소를 뒷받침하고 국가적 접근 방식으로 통합하는 사이버 전력의 토대가 되는 요소
- 사이버 공간이 시민과 경제에 제공하는 모든 이점을 실현하기 위해 사이버 보안과 복원력을 통해 우리의 자산을 보호하는 능력
- 핵심 사이버 기술의 진전에 있어서 주도권을 유지하고 사회의 이익이 되도록 새로운 발전을 전개하기 위한 기술 및 산업 역량
- 사이버 공간에서 우리의 가치와 이익에 맞춰 규칙과 규범을 설정하고 국제 안보와 안정을 증진하기 위한 세계적 영향력, 관계 및 윤리 규범
- 국가 안보, 경제 복지 및 범죄 예방을 지원하기 위해 사이버 공간을 통해 조치를 취할 수 있는 능력. 여기에는 현실 세계 효과를 경험하게 하는 사이버 활동과 전략적 이점을 선점하도록 돕는 일, 악성 사이버 범죄자를 활동을 제재하고 저지하기 위해 법을 집행하고 적용하는 것을 포함한다

13. 사이버 전력은 전통적 형태의 역량과는 구별된다. 사이버 전력은 강력한 역량과 보다 부드러운 영향력의 지렛대의 완벽한 조합을 필요로 한다. 사이버 전력은 기존의 역량과는 달리 광범위하게 분배되어 있어서 정부는 이 힘을 행사하기 위해 파트너들과 협력해야 한다. 또한 사이버 전력은 기존의 최첨단 능력이 새로운 발전으로 인해 쉽게 쓸모가 없어지는 것처럼 빠른 기술 변화 속도의 영향을 받아 쉽게 얻고 잃을 수 있다.

14. 우리의 전략은 상기 사항을 반영하여, 사회 전체의 노력을 일환으로 가능한 분야에서는 최대한 파트너와 협력하는 방법을 포함하고 있다. 우리는 초기에 발생하는 문제들을 제시하고 근본적인 원인을 고치고, 향후 동향을 예측하고 장기적인 대응 방안을 마련하며, 수동적 대응하기보다는 경쟁적 지정학적 환경을 적극적으로 만들어 갈 것이다.

현재의 사이버 파워로서의 영국

15. 영국은 이미 선도적인 사이버 강국이다.[1] 지난 10년 동안 정부는 영국의 사이버 보안을 강화하고, 사이버 위험에 대한 대중의 인식을 높이고, 사이버 보안 분야를 성장시키고, 사이버 공간을 통해 적대자들의 위협에 대응하기 위한 광범위한 능력을 개발하기 위한 지속적인 국가적 노력을 다해 왔다. 우리는 큰 발전을 이루었고 확고한 입지를 다졌지만 이 전략의 5대 핵심 축에 걸쳐 여전히 중요한 어려움에 직면해 있다.

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

영국의 사이버 생태계 및 기술 리더십

16. 영국은 국가적 사이버 기술 기반과 상업적 역량을 개발하기 위한 협력을 영국 정부와 북아일랜드, 스코틀랜드, 웨일스의 정부와 함께 해 왔고 이로 인하여 서로에게 배우고 있다. 영국 사이버 보안 분야는 지난해 1400여 개 기업이 89억 파운드의 수익을 창출하고 4만 6700개의 일자리를 지원하며 상당한 해외 투자를 유치하는 등 빠르게 성장하고 있다. 이 분야는 우리의 사이버 파워, 우리의 안보를 지원하고, 그리고 국제적인 영향력과 경제 성장에 필수적이다. 영국은 19개의 우수 교육 센터와 4개의 연구소가 우리의 가장 시급한 사이버 보안 과제를 해결하면서 사이버 보안 연구의 글로벌 리더로서의 명성을 굳건히 했다.

17. 사이버 보안 부문 인력은 지난 4년 동안 약 50% 증가했으며, 기술을 갖춘 인력의 수요가 공급을 앞지르는 경우가 많았다. 우리는 사이버 보안 기술력을 갖추기 위한 어려움의 본질을 더 잘 이해하기 위해 산업, 전문 기관, 학생, 고용주, 기존 사이버 보안 전문가 및 학계와 광범위하게 협력하고 있다. 우리는 청년들이 사이버 보안 분야에서 경력을 쌓도록 격려하기 위해 광범위한 정식 학과 외의 교육 과정을 개발했다. 2019년부터 2020년까지 CyberFirst 및 Cyber Discovery 학습 프로그램에 57,000명에 가까운 청년을 참여시켰다. 우리는 어린 학생들에게 더욱더 다가갈 수 있도록 교육 과정을 확장했고, CyberFirst Girls' 온라인 대회는 11,900명의 여학생들이 참가했으며, 영국 전역의 18개 장소에서 상위 팀들이 동시에 경쟁했다. 우리의 CyberFirst 장학 프로그램에는 재능과 열의가 있는 학부생들이 지원하여 작년에는 750명의 학생들이 이 참여했고 56명의 석사 학위자들이 모두 사이버 보안 분야에서 정규직으로 일하고 있다.

18. 이러한 노력에도 불구하고 숙련된 인적 자원 공급은 여전히 상당한 과제에 직면해 있다. 전체 경제의 132만 개의 기업 중 약 50%가 여전히 기본적인 사이버 보안 기술 인력의 부족을 보고하고 있다.[2] 그리고 영국의 사이버 보안 분야는 빠르게 성장했지만, 이 분야의 대부분의 기업은 스타트업이고, 국제적 합병이 필요한 가운데 국내 대규모 업체를 설립하는 것은 여전히 어려운 과제이다. 5G에서의 사례에서도 보았듯이, 영국과 동맹국들은 광의의 기술 산업의 일부 핵심 분야에서 선두적인 위치를 차지하고 있지 않다. 사이버 파워에 중요한 기술에서 선도적 역할을 확립해야 설계 및 구축 방식에 영향을 미칠 수 있는 위치를 확보하고, 보안 및 경제적 이점을 더 잘 보존할 수 있으며, 사이버 능력의 획기적인 발전을 위한 기회를 더 빨리 활용할 수 있을 것이다.

영국의 사이버 복원력

19. 지난 10년 동안 우리는 영국의 사이버 복원력을 강화하기 위한 광범위한 조정을 해왔다. 이는 NCSC (국가 사이버 보안 센터), 법 집행 기관, 정부 전반의 보안 및 정책 전문가, 국내외 파트너십 확대 등 우리의 핵심 사이버 역량에 대한 의미있고 지속적인 투자 덕분에 가능했다.

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

20. 우리의 가장 혁신적이고 획기적인 노력은 Active Cyber Defence (ACD) 프로그램의 개발과 공식 발표를 포함한 활동이었다. 지난 해에는 국민 건강 보험 브랜드를 이용한 442건의 피싱 캠페인과 공식 앱스토어가 아닌 곳에서 호스팅 및 다운로드할 수 있는 80건의 불법 국민 건강 보험 앱을 포함하여 230만 건의 악성 캠페인을 제거했다.[3] 또한 우리는 연결 가능한 소비자 제품이 '안전하게 설계되도록' 하는 전세계적으로 추진하였고, 2018년에는 영국 실천 강령을 개발하여 인터넷 연결 소비자 제품에 관하여 최초로 세계적으로 적용 가능한 산업 기준을 알리고 따를 수 있게 하였다.[4, 5]

21. 새로운 규제를 만들어 사이버 보안에 긍정적인 영향을 미쳤고, 82% 의 기관들이 2018년 영국 일반 데이터 보호 규정의 도입에 영향을 받아 개선점을 만들수 있었다고 응답하였다.[6] 또한 기업의 77%가 현재 사이버 보안을 최우선 과제로 보고 있으며, 이는 2016년 이후 12% 증가한 수치다.[7] 2018년 네트워크 & 정보 시스템 규정('NIS 규정')의 도입으로 지정된 기관들은 네트워크와 정보 시스템의 보안을 보장하기 위한 조치를 취하여 필수 서비스와 중요한 디지털 서비스에 대한 사이버 위험을 감소시켰다.[8] 영국 4개국 협력의 좋은 예로서 보건 분야 전반에 걸쳐 NIS 규정의 시행을 포함한 많은 개선을 이룬 것을 들 수 있다.

22. 우리는 광범위한 경제의 조직에 포괄적인 사이버 보안 조언과 지침을 제공하고 코로나 바이러스 (COVID-19) 팬데믹 시대에 중요한 부문에 대한 맞춤형 지원을 제공해 왔다. 일반 대중을 위해서는 우리의 사이버 인식 캠페인을 실시하여 온라인에서 그들 자신을 보호하기 위해 취할 수 있는 방법에 대해 조언을 제공했다. 사이버 공격이 발생했을 때, 우리는 세계 최고의 사건 대응 능력을 활용하여 가장 심각한 사건에 대해 직접적인 지원이 가능하도록 하였고 지역 법 집행 전문가에게 투자한 덕분에 모든 신고 사건에 대해 대응할 수 있게 되었다.

23. 우리는 영국에 전문 법률 집행 기관 사이버 부서를 설립했고, 이와 함께 사이버 보호 네트워크, 경제 범죄 피해자 대응 부서 및 지역 사이버 복원 센터를 설립했다. 이것은 일반 국민과 중소 기업은 사이버 복원력 향상을 위한 지원 및 지침을 제공할 수 있는 적절한 기술과 현지 지식을 보유한 사람이 근처에 있거나 쉽게 연락할 수 있음을 의미한다.

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

24. 그러나 사기 사건과 같은 사이버 기반 범죄 뿐만 아니라 정부, 기업 및 개인에 영향을 미치는 사이버 범죄의 수준 및 위반이 계속 증가함에 따라 국가 복원력의 취약성이 존재함을 알 수 있다.[9, 10] 전통 IT 시스템, 공급망 취약성 및 사이버 보안 전문가 부족에 대한 우려가 커지고 있다. 거의 10개 중 4개의 기업(39%)과 1/4의 자선단체 기업(26%)이 작년에 사이버 보안 침해 또는 공격을 당했다고 보고했으며, 많은 기관(특히 중소기업)은 스스로를 보호하고 사고에 대응할 능력이 부족하다.[11] 업계에서는 많은 기업이 당면한 사이버 위험을 인지하지 못하고 있으며, 사이버 보안에 투자할 상업적 이익이 명확하지 않으며, 침해와 공격을 관련 기관에 보고할 동기가 부족한 경우가 많다고 한다.

영국의 국제적 리더십과 영향력

25. 국제적으로, 영국의 사이버 전문 지식은 우리의 파트너들이 높이 평가하고 있으며, 영국은 악의적인 사이버 활동에 맞서기 위해 국제적인 능력을 향상시키고 해결하는데 있어 중요한 역할을 해왔다. 이는 일부 적대국의 무분별한 활동과 대조적으로 영국과 국제법 및 공식적 입장과 일관되게 우리의 공격적 사이버 능력을 정당하게 사용함으로써 강고히 되었다.

26. 영연방의 의장 재임 기간 동안 영국은 사이버 공간에서 우리의 안보, 번영, 가치에 대한 공동의 약속인 영연방의 사이버 선언의 이행을 구상하고 주도했다. 국가 범죄청 (NCA) 국제 네트워크는 오랜 협업적 대응의 역사를 통해 다져진 관계를 바탕으로 국외 사이버 법률 집행 기관과의 파트너십을 강화했다. 영국은 또한 5개 대륙에 걸쳐 사이버 및 기술 보안 담당자들의 해외 네트워크를 성장시키고, 100개국에 걸쳐 역량 구축 사업을 수행함으로써 복원력을 형성하고, 영국의 영향력을 강화하고, 영국이 지향하는 가치를 홍보하여 왔다.

27. 사이버 보안 대사 프로그램을 통해 장기적인 관계를 발전시키고, 영국 기업들이 주요 국제 계약을 성사할 수 있도록 도움을 주어왔다. 영국은 디지털 액세스 프로그램과 같은 국제 개발 사업을 중재함으로써 아프리카, 아시아 및 라틴 아메리카의 협력국들과 성공적으로 협업하여 이들 국가의 정부, 비즈니스 부문 및 사용자의 사이버 보안 역량을 개발하였다. 그리하여, 가장 보안이 취약한 커뮤니티의 온라인 상의 리스크와 과제로부터 보호 할 수 있는 사이버 보안 능력을 증진 시켰다.

28. 그러나 중국과 러시아와 같은 조직적 경쟁자들이 보안 문제에 대한 해답으로 사이버 공간에 대한 더 큰 국가 통치권을 계속해서 제시하고 있기 때문에 우리는 국제적으로 경쟁을 직면하고 있다. 인터넷 상 자유는 세계적으로 감소하고 있으며 개방된 사회 간의 지식과 재화의 교류를 지원하는 공유 공간으로서의 인터넷의 미래는 위협받고 있다.

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

영국에 대한 사이버 위협에 대응과 적대 행위의 저지

29. 우리가 사이버 공간에서 그리고 사이버 공간을 통해 직면하는 위협들은 최근 몇 년간 강도, 복잡성, 심각성의 모든 면에서 증가해 왔다. 영국에 대한 사이버 공격은 광범위한 정부 소속 요원, 범죄 단체 (때로는 주 정부의 지시에 따라 행동하거나 암묵적인 승인을 받아 행동) 및 활동가들이 스파이 활동, 상업적 이익, 사보타주 및 허위 정보를 목적으로 행해진다. 이러한 공격은 상당한 재정적 손실, 지적 재산 도난, 심리적 고통, 서비스와 자산의 중단 및 우리의 중요한 국가 기반 구조, 민주주의 기관 및 미디어에 대한 위험을 야기한다. 또한 투자자와 소비자의 신뢰도를 손상시키고 기존의 불평등과 피해를 증폭시킬 수 있다. COVID-19 대유행 기간 동안 성별 기반 폭력의 유사 대유행은 온라인 공격에 의해 심화되었다. 랜섬웨어 공격은 갈수록 정교해지고 피해가 커지고 있다. COVID-19 대유행 기간 동안 적대적 행위자들의 사이버 위협의 전반적인 수준은 일정하게 유지되었지만, 그들은 그것을 기회로 삼아 백신과 의학 연구를 훔치고 위기로 인해 이미 어려움을 겪고 있는 다른 국가들을 약화시키기 위한 사이버 운영으로 전환했다. 원격 근무 및 온라인 거래를 위한 디지털 기술에 대한 의존도가 높아지면서 위험에 대한 노출도 증가하고 있다. 이와 함께, 디지털 격차는 온라인 서비스에 대한 불공정한 접근성을 갖게 했고, 제한된 디지털 사용 능력과 온라인 보안을 유지하기 위해 우리가 취할 수 있는 사이버 보안 조치에 대한 인식의 한계로 온라인 남용과 위해에 노출되었다.[12]

30. 정부는 이러한 증가하는 위협에 대응하기 위한 조치를 취해 왔다. 첩보 기능에 대한 상당한 투자를 통해 위협에 대한 이해를 높혔으며 보다 효과적인 은신처 대응 작전을 실시할 수 있었습니다. 우리는 국가범죄청 (NCA)과 잉글랜드, 웨일즈, 북아일랜드 및 스코틀랜드 전역의 지역 조직 범죄단 및 지역 경찰 내 전담 사이버 팀을 주축으로 사이버 범죄에 대한 통합 법 집행 팀을 개발했다. 이것은 사이버 범죄자와 다른 적들에 대한 우리의 작전 및 수사적 우위를 강화했다. 정부는 또한 영국의 디지털 아이덴티티 및 속성 신뢰 프레임워크를 개발함으로써 증가하는 디지털 아이덴티티 솔루션의 보안을 강화하고 있다.[13] 이것은 또한 신원 데이터의 오남용을 포함하는 범죄를 해결하는 데 도움이 될 것이다. 그리고 NCA의 사이버 선택 프로그램(Cyber Choices Programme)은 사람들이 더 많은 정보에 입각한 선택을 하도록 돕고 있으며, 그들의 사이버 능력을 범죄가 아닌 긍정적이고 합법적인 방법으로 사용할 수 있도록 하고 있다.

31. 우리는 첫째, 국가 공격적 사이버 프로그램 (National Offensive Cyber Programme)을 통해, 그리고 더 최근에는 국가 사이버군(NCF)의 설립을 통해 우리의 공격적 사이버 역량에 상당한 투자를 해왔다. NCF는 정부통신본부 (GCHQ), 국방부 (MOD), 비밀정보국 (SIS), 국방과학기술연구소(MI6)의 인원을 처음으로 하나의 통일된 사령부로 모이게 하였다. 이들은 국가를 안전하게 지키고 국내외에서 영국의 이익을 보호하고 증진시키기 위해 사이버 공간에서 그리고 사이버 공간을 통해 운용되고 있다.

[12] NCSC, CyberAware ↩
[13] DCMS, UK digital identity and attributes trust framework (2021)

32. 또한 동맹국들과 협력하여 최근 SolarWinds 및 Microsoft Exchange 위반 사건에서와 같이 사이버 공간에서 국가가 지원하는 적대적 활동의 비용을 높이고 책임자들에게 그에 따른 책임을 지도록 하는 방안을 모색하고 있습니다. 영국의 자율적인 사이버 제재 체제를 개발하여 워너크라이, 노트페티아 공격과 같은 사건에 대응하기 위해 우리가 사용해 온 또 하나의 상대를 와해할 수 있는 도구를 추가했다. 그러나, 이 모든 것에도 불구하고, 사이버 억제에 대한 우리의 접근 방식으로 아직 공격자들의 리스크 계산법을 근본적으로 바꾸지 못한 것으로 보인다. 중대한 사이버 공격의 몇 가지 최근 예가 아래에 설명되어 있다.

사이버 공격에 대한 최근 사례 연구

2021년 동안 영국은 대부분 러시아나 중국에서 지속적으로 발생하는 공동의 위협을 탐지하고 저지하기 위해 글로벌 파트너들과 계속 협력했다. 러시아 정부가 제기하는 직접적인 사이버 보안 위협 외에도, 서방 국가들을 대상으로 랜섬웨어 공격을 감행하는 범죄 조직들 중 많은 숫자가 러시아에 근거지를 두고 있다는 것이 명백해졌다. 중국은 국경을 넘는 영향력을 행사하려는 야망과 영국 상업 비밀에 대한 명백한 관심을 보이며 사이버 공간에서 매우 수준 높은 활동을 하고 있다. 중국이 향후 10년 동안 어떻게 발전하는가는 아마도 영국의 미래 사이버 보안의 가장 큰 위협이 될 것이다. 이란과 북한은 러시아나 중국보다는 수준 높진 않지만, 그들의 목적을 달성하기 위해 절도와 방해 행위를 포함한 디지털 침범을 계속 시도하고 있다.

랜섬웨어를 사용하여 공공 서비스를 공격하는 사이버 범죄자

랜섬웨어는 2021년 영국이 직면한 가장 중대한 사이버 위협이 되었다. NCSC는 랜섬웨어가 국가 지원 스파이만큼 잠재적으로 유해하다고 평가했다.[14]

2020년 10월, 해크니 의회는 랜섬웨어 사이버 공격을 받았고, 이로 인해 수개월간 운영 중단이 발생했으며, 이를 해결하기 위해 수백만 파운드가 소요되었다. COVID-19 확산으로 조치를 취해야 하는 중요한 시기에 위원회의 중요한 데이터가 차단되었고 의회 세금과 혜택 지급을 포함한 많은 서비스가 중단되었다. 다른 지방 정부들도 비슷한 공격을 받았고, 교육 분야의 여러 기관들도 마찬가지였다.

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

2021년 5월 아일랜드 보건 서비스 집행부(HSE)에 대한 랜섬웨어 공격으로 10일 넘게 아일랜드 의료 IT 네트워크와 병원이 마비되면서 환자와 그 가족에게 실질적인 피해가 발생했다. 도난당한 환자 데이터가 온라인에 게시됐다. 아일랜드에서 보건 및 사회 복지 서비스를 제공하는 HSE는 이 사건에 대응하기 위해 국가 및 지역 네트워크를 같은 날 폐쇄했다. 아일랜드 보건부(DoH) 네트워크에서도 악성 사이버 활동이 감지됐으나 조사 과정에서 툴을 배치하면서 랜섬웨어 실행 시도가 적발돼 중단됐다. 이 공격은 HSE가 보유한 국경 넘어의 환자 서비스 데이터에 액세스할 수 있는 능력에도 영향을 미치며 북아일랜드에 충격을 주었다.

중요한 것은 두 경우 모두 몸값이 지급되지 않았다는 점이다. **법률 집행 기관은 몸값 지불을 권장하거나 보증하거나 용납하지 않는다. 몸값을 지불하면:**

- **당신이 당신의 데이터나 컴퓨터에 접근할 수 있다는 보장은 없다**
- **당신의 컴퓨터는 여전히 감염되어 있을 것이다**
- **당신은 범죄 집단에 돈을 지불하는 것이 될 것이다**
- **미래에 또 공격의 목표가 될 가능성이 더 높다**

NCSC에서는 사고에 대비하는 방법과 기관이 이미 감염된 경우 취해야 할 조치를 포함하여 악성 소프트웨어 또는 랜섬웨어 공격으로부터 기관을 보호하는 방법에 대한 지침을 제공한다.

전략적 취약점과 공급망을 이용하는 국가

소프트웨어 회사인 SolarWinds에 대한 공격과 Microsoft Exchange Server의 악용은 공급망 공격으로 인해 어떤 위협이 가능한지를 조명하였다. 위의 두 사건은 경제, 정부 및 국가 보안 기관의 공급망에서 관리형 서비스 제공 업체나 상업용 소프트웨어 플랫폼과 같은 덜 안전한 요소를 목표로 삼은 이러한 정교한 공격 활동은 NCSC가 관측한 가장 심각한 사이버 침입이었다.

2020년 12월 초, 미국의 사이버 보안 회사인 FireEye는 공격자가 자사와 전 세계의 많은 기관이 사용하는 제품에 악의적인 수정을 추가할 수 있다는 것을 발견했다. 이 수정은 공격자가 관리자 수준의 명령을 감염 설치가 완료된 제품에 보낼 수 있게 해주었고 연결된 시스템에 대한 추가적인 공격을 가능하게 했다. 초기의 공급망 공격은 SolarWinds라는 회사가 개발한 IT 네트워크 모니터링 도구인 Orion이라는 소프트웨어를 통해 이루어졌다. 이 활동은 2020년 3월, 소프트웨어 업데이트 파일에 악성 코드를 이식하는 것부터 시작 되었다. 2021년 4월, NCSC는 미국의 보안 담당자들과 함께 러시아 대외정보국(SVR)이 근래에 있던 가장 심각한 사이버 침해인 이번 공격의 배후임을 처음으로 밝혔다.[15] SolarWinds는 미국 정부 부서를 포함한 전 세계 18,000개 기관이 피해를 입었다고 확인했다. 이 사건은 이전에 NATO 회원국과 유럽 전역의 정부들의 IT 네트워크에 접근하려고 시도했던 SVR에 의한 광범위 사이버 침입의 일부였다.

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

2021년 3월 2일, Microsoft는 정교한 적들이 전 세계 기관들이 이메일, 일정, 협업을 관리하기 위해 사용하는 수많은 **Microsoft Exchange** 서버를 공격했다고 밝혔다. Microsoft는 초기 침입이 2021년 1월부터 시작되었으며 중국 정부의 지원을 받은 것으로 평가했다. 이에 대응하여 감염된 서버에 대한 여러 보안 업데이트를 출시했다. 2021년 7월, 영국은 같은 생각을 가진 파트너 국가들과 중국 정부의 지원을 받는 적들이 전세계 25만개 이상의 서버 침해 공격에 책임이 있다는 것을 공식화 했다.[16] 이번 공격은 개인 신상 정보와 지적 재산 획득을 포함한 대규모 스파이 활동을 가능케 할 가능성이 매우 높았다. Microsoft Exchange에의 공격으로 가해자는 피해자들의 IT 네트워크에서 더 깊이 활동할 수 있는 발판을 마련했다. 공격 당시 정부는 피해자들에게 신속한 조언을 통해 조치를 권고했으며 Microsoft는 3월 말까지 고객의 92%가 취약점을 해결하기 위한 패치를 했다고 밝혔다.

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

변화의 원동력

33. 향후 10년간 우리 삶의 거의 모든 측면에서 데이터의 급속한 확장과 디지털 결합은 계속될 것이다. 데이터와 데이터 사용에 의존하는 인프라에 의해 뒷받침되는 인터넷 액세스와 사용의 거대한 전 세계적인 성장은 새로운 시장을 창출하고 편의성, 선택권 및 효율성을 높이고 있다. 그러나 이는 또한 국가들이 상호 연결된 디지털 시스템에 훨씬 더 많이 의존하게 만들어 악성 활동과 심각한 '현실 세계' 영향을 받을 수 있는 더 많은 기회를 제공한다. 필수 기술과 비필수 기술이 여러 부문에 걸쳐 계속 융합됨에 따라 이러한 리스크는 경제의 새로운 영역으로 확산되고 있으며, 데이터와 서비스가 클라우드와 때로는 영국 외부로 이동함에 따라 우리는 리스크에 노출되고 있다.

34. 우리는 통신 및 에너지와 같은 규제 부문의 기존 사업체와 자가 전력, 전기차 충전 또는 '연결된 장소' 기능을 제공하는 신규 및 비규제 부문 사업체의 상호 작용을 점점 더 많이 목격하고 있다. 중요 인프라는 훨씬 더 널리 퍼지고 확산될 것이며, 이는 근본적으로 규제가 우리가 의존하는 중요한 기능과 서비스의 보안에 미치는 영향을 변화시킬 것이다. 이러한 다양화는 우리의 더 넓은 범위의 국가 안보에도 영향을 미칠 것이며, 법률 집행이든 사이버 보안이든 정보에 접근하는 것을 더 어렵게 만들 것이다. 이러한 환경의 변화는 전통적 중요 국가 기반 시설 뿐 만 아니라 더욱 광범위한 제품과 서비스에 영향을 미칠 것이다.

35. 이렇게 점점 복잡해지는 환경으로 국가, 기업 및 사회가 직면한 위험과 스스로를 보호할 수 있고 보호해야 하는 방법을 인지하는 것을 더욱 어렵게 만들 것이다. 수천 명의 고객의 IT 시스템에 대한 특권을 가지고 있는 관리형 서비스의 제3자 공급 업체에 대한 의존도가 높아짐에 따라 해결해야 할 새로운 리스크가 발생하고 있다. 기기와 네트워크는 점점 더 인터넷에 연결되는 것이 표준이 되어 사이버 공간이 우리의 가정, 자동차, 환경 및 산업 인프라로 확장할 것이다. 센서, 착용 기기, 의료 기기 및 생체 인식은 오프라인과 온라인 활동의 경계를 더욱 불분명하게 만들 것이다. 사이버 리스크가 만연하여 생성되는 개인 및 민감한 데이터의 양과 시스템이 침해될 경우 잠재적인 충격이 증가할 것이다.

36. 이러한 배경에서 **사이버 공간의 위협은** 고급 사이버 기능이 상품화되고 더 광범위한 국가 단위 및 범죄 집단으로 확산됨에 따라 **계속 진화하고 다양해질 것이다.** 사이버 공간에서 능력을 가지고 영국을 타깃으로 삼는 활동가들의 수가 증가할 것이고, 국가는 대리인들의 이용을 포함한 파괴적인 활동을 하기 위해 더 다양한 수단을 사용할 것이다. Covid-19로 인한 하이브리드 근무와 해외 여행에 대한 제약의 급격한 변화는 디지털 서비스에 대한 의존도를 높이고 체계적인 범죄 집단이 사이버 범죄에 악용할 수 있도록 만들었다. 우리는 이미 이러한 추세를 2019년부터 2021년 사이에 범죄가 크게 증가한 것으로 추정하는 최근 범죄 설문을 통해 접하고 있다.[17]

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

이 과제는 영국에만 국한되지 않고 사이버 공간에 의존하는 모든 사람들에게 공동의 취약성을 부여하고 있다.

37. 국가와 비국가 활동가들이 사이버 공간에서 그리고 사이버 공간을 통해 전략적 우위를 추구함에 따라 사이버 공간은 더욱 경쟁적으로 될 것이다. 사이버 작전은 무장 충돌 및 분쟁 이전에 전력 예측을 위해 점점 더 중요해질 것이다. 앞으로 발생할 분쟁에서 역시 사이버 능력 사용이 증가할 것이다. 영국이 효과적으로 활동하기 위해서는 우리의 방어 체제 능력에 있어서 더 높은 수준의 사이버 복원력을 필요로 할 것이다. 사이버 작전은 위협을 물리치고 더 넓은 방어 활동을 하기 위해 다른 군사 요소와 통합되어야 할 것이다. 국가 우주 전략에서 규정한 바와 같이, 우주 공간도 점 점 더 활동의 영역이 되어 새로운 위험 분야를 야기할 뿐만 아니라 영국이 사이버 능력을 이용하여 새로운 방식의 이점을 성취해낼 수 있는 기회를 창출할 것이다.[18]

38. 사이버 공간을 지배하는 규칙에 대한 논쟁은 점점 더 **강대국들 간의 체계적 경쟁**의 현장이 될 것이며, 사이버 공간을 확보하기 위한 유일한 방법으로 더 큰 국가 통제를 주장하는 러시아와 중국 같은 체계적인 경쟁자들과 개방 사회에서 시스템을 보호하려는 국가들 간의 가치 충돌로 이어질 것이다. 이것은 자유롭고 개방적인 인터넷에 압력을 가할 것이며, 국가, 거대 기술 회사 및 기타 활동가들의 기술 표준과 인터넷 정책에 대한 경쟁적 접근법을 취하게 되기 때문이다.

39. 이러한 상황은 **빠르게 진화하는 기술 환경에 대한 통제 경쟁**으로 인해 더욱 악화될 것이다. 디지털 기술이 우리의 일상, 비즈니스 및 인프라에 통합되면서 일부 기술은 사회의 기능에 굉장히 중요한 요소가 되고 있다. 권력은 점점 더 과학과 기술에서 전략적 우위를 점하는 국가들에게, 그리고 혁신을 이끄는 데이터에 접근하여 다른 국가에 영향력을 행사하고 자국의 경제적, 정치적 이익에 가장 부합하는 방식으로 글로벌 기준을 형성할 수 있도록 하는 국가들에게 집중될 것이다.

40. 디지털 트윈, 양자 컴퓨팅, 대규모 자율 시스템과 같은 신흥 기술과 이들이 생성하는 정보는 랜섬웨어 범죄 조직에 의해 암호화폐가 악용되고 있는 것처럼 새로운 사이버 기능을 제공하여 공격자와 방어자에게 새로운 기회와 위험을 창출할 것이다. 기술 리더십은 점점 분산되고 있고, 영국은 중요한 모든 기술에서 주권 능력을 키울 수 없을 것이다. 국가와 기업은 자신의 이익을 증진하기 위해 기술 기준을 형성하고 우리의 가치를 공유하지 않는 사람들에 의해 형성되는 핵심 기술은 위험요소가 될 것이다.

41. 10년 이상 영국은 야심찬 국가 사이버 보안 전략을 추구해 왔으며 상당한 수준의 투자를 지속하여 사이버 분야의 글로벌 리더로 자리매김했다. 위의 분석에서 알 수 있듯이, 중대한 과제와 기회가 남아 있다. 다음 섹션에서는 우리의 국가적 대응에 대해 설명한다.

[18] HMG, National Space Strategy (2021)


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

우리의 국가적 대응

42. 이런 전략적인 환경에서 영국은 선택을 해야 한다. 우리는 지난 5년간의 과정을 통합하고 우리가 할 수 있는 한 가장 시급한 문제들을 해결하면서, 점점 더 복잡해지는 사이버 공간에서 직면하는 위협과 도전의 속도를 맞춰 가는 것 만을 목표로 할 수 있다. 그러나 이러한 접근에는 두 가지 리스크가 있다. 첫 번째는 국가 우선 순위를 지원하기 위한 영국의 사이버 강점의 잠재력을 완전히 깨닫지 못하고 기회를 놓칠 수 있다는 것이다. 두 번째로, 더 심각한 리스크는 우리는 기술적 절벽에 다다르게 되고, 우리의 미래 경제와 사회의 토대가 우리의 경쟁자들과 적들에 의해 형성되는 상황을 맞게 되어 결국 우리의 안전을 보장하기 위해서는 더 많은 노력해야 할 것이라는 것이다.

43. 우리의 판단으로는 점점 더 사이버 공간이 우리의 이익과 동맹과 적대국의 이익에 핵심이 되어 감에 따라, **이러한 환경을 다루는 데 있어서 우리의 경쟁적 이점을 발전시키는 것이 전략적으로 필수적이라는 것이다.** 그리하여 오늘날 우리의 안전을 보장할 뿐만 아니라 미래의 세계를 형성하고 그로부터 이익을 얻을 수 있게 될 것이라는 것이다.

우리의 비전, 목표 및 원칙

44. 우리의 비전은 2030년에도 영국이 **국가 목표를 지원하며 사이버 공간과 사이버 공간을 통해 우리의 이익을 보호하고 증진시킬 수 있는 책임감 있고 민주적인 사이버 강국이 될 것이라는 것이다.**

45. 이 비전을 실현하기 위해 우리는 다섯 가지 전략적 목표를 추구할 것이다. 각각의 목표는 사이버 전력의 다섯 가지 관점 중 하나에서 우리의 국력을 강화하는 것을 목표로 하고 있으며, 종합적으로 우리의가치와 이익을 반영한 사이버 공간을 유지하는 능력을 높이는 것을 목표로 하고 있다. 이 다섯 가지 목표(또는 전략 축)는 우리의 활동의 방향을 제시하는 전략적 틀을 형성하며, 2장에서는 각각의 목표 하에서 2025년까지 우리가 취할 행동들을 설명한다.

- **전략 축1:** 우리 인력과 기술에 대한 투자, 정부, 학계, 산업계의 파트너십 심화함으로써, **영국의 사이버 생태계 강화**

- **전략 축2:** 기업이 디지털 기술의 경제적 이익을 극대화하고, 시민이 온라인에서 데이터를 안전하게 보호할 수 있도록 사이버 위험 감소함으로써, 복원력 있고 번영하는 디지털 영국 구축

- **전략 축3:** 산업 역량 구축 및 미래 기술 확보를 위한 프레임워크 개발함으로써, 사이버 전력에 필수적인 기술 선도

- **전략 축 4:** 정부 및 산업 파트너와 협력하고 영국의 사이버 전력을 뒷받침하는 전문 지식을 공유함으로써, 보다 안전하고 번영하며 개방적인 국제 질서를 위한 영국의 글로벌 리더십과 영향력 향상.

- **전략 축 5:** 영국의 모든 범위의 수단들을 보다 통합적이고 창의적이며 일상적으로 사용함으로써, **영국의 보안을 강화하기 위해 사이버 공간에서 그리고 사이버 공간을 통해 적들을 감지, 방해 및 저지**

46. 이 목표들은 상호 강화되도록 설정하였다. 예를 들어, 국내에서 더 높은 수준의 사이버 보안과 복원력을 달성하는 것은 국제적으로 더 적극적인 입장을 취하는 데 필요한 기반이 될 것이다. 그리하여 우리의 글로벌 공급망과 해외로부터의 위협은 국제 활동가들의 행동 양식을 보다 적극적으로 파악하지 않고는 우리 자신의 안전을 보장할 수 없다는 것을 의미한다. 그리고 우리의 기술적 우위 유지와 가장 중요한 기술에서 진정한 이점을 창출하는 혁신 생태계를 구축할 수 있느냐에 따라 우리가 사이버 공간, 인터넷 및 기술에 관한 국제적 논쟁에서 영향을 미칠 수 있는 능력을 가질 수 있는가를 결정하게 될 것이다.

47. 우리의 비전에서 가장 중요한 것은 **사이버 공간을 더 자유롭고 개방적이며 평화롭고 안전하게 하는 것이다.** 사이버 전력에 대한 우리의 전략적 초점은 갈등을 유발하거나 영국이 제로섬 게임 (이득과 합이 0이 되는 게임)에서 이기도록 하는 것이 아니다. 통합 검토서(IR)에서 밝힌 바와 같이 열린 사회와 경제가 번창할 수 있는 세상이 우리의 미래 번영과 주권, 안보를 가장 잘 담보해 줄 것이다. 영국은 사이버 파워에 대한 책임감 있고 민주적이면서 개방성과 민주주의라는 공동의 가치를 증진시키기 위해 같은 생각을 가진 국가들과 협력할 것이다. 우리는 다섯 가지 전략적 목표를 달성하기 위해 다음 **원칙**들을 적용할 것이다:

- 우리는 국민과 기업이 사이버 공간에서 안전하게 운영할 수 있는 능력을 우선시 하여 디지털 기술의 경제적, 사회적 이익을 극대화하고 법적, 민주적 권리를 행사할 수 있도록 할 것이다.

- 우리는 개방적이고 상호 정보 교환이 가능한 인터넷을 유지하기 위해 노력하여 세계적인 번영과 복지를 지지하고 독재적인 국가들의 분리주의와 인터넷 주권에 대한 그들의 압력에 저항할 것이다.

- 우리는 공공과 우리의 동맹에 대한 명확한 관리와 협력 하에 사이버 능력을 합법적이고 비례적이며 책임감 있게 사용할 것이며, 사이버 공간에서 무모하거나 무차별적인 행동에 대한 책임을 물을 것이다.

- 사이버 공간을 범죄적으로 사용하는 것에 모든 수단을 동원하여 조치를 취할 것이며, 범죄 대리인을 부르거나 범죄 집단을 자신의 지역에 숨겨주는 사람을 찾아내고 고급 사이버 능력을 범죄에 사용하는 것이 확산하는 것을 막기 위해 노력할 것이다.

- 우리는 사이버 공간과 디지털 기술의 미래에 대한 논쟁에 대한 포괄적, 다중 이해당사자 접근을 옹호할 것이며, 사이버 공간에서 인권을 지지하고 디지털 권위주의와 국가 통제를 향한 움직임에 대항할 것이다.

우리의 접근 방식의 주요 변화

48. 많은 영역에서 우리의 전략은 현재의 접근 방식을 기반으로 하며, 필요한 경우 우리의 노력을 강화, 확장 또는 조정하고자 한다. 2016-2021년 국가 사이버 보안 전략과의 주요 차이점은 다음과 같으며, 선도적인 사이버 강국으로서 영국의 입지를 공고히 하려는 우리의 더 야심찬 의지를 반영한다.

49. 사이버 관련해서 영국을 최선두에 두기 위한 의지. 정부는 향후 3년간 사이버와 레거시 IT에 26억 파운드를 투자할 예정이다. 이는 국가 사이버 군(National Cyber Force)이 발표한 2020년 예산 검토(SR20)에서 발표한 예산와는 별도의 예산 투자이다. 여기에는 국가 사이버 보안 프로그램의 1억 1,400만 파운드의 추가 투자를 포함하고 있으며, 연구 개발 (R&D), 기밀, 국방, 혁신, 인프라 및 기술에 대한 투자 증가와 함께 영국의 사이버 전력에 기여할 것이다. 2020년 및 2021 예산 검토(SR21)에 발표된 사이버 투자액은 이전 전략에 입각한 5년간 19억 파운드를 훨씬 초과하는 예산이다.[19]

50. 더 종합적인 국가 사이버 전략. 사이버 보안은 여전히 이 전략의 핵심이며, 정부 안팎에서 영국의 모든 역량을 하나로 모으고 있다. 사이버 공간을 뒷받침하는 중요한 기술과 인프라에 더 큰 비중을 두고, 영국의 사이버 기업들이 국내 성장과 국제적으로 경쟁할 수 있도록 지원하고, 사이버 공간의 미래를 형성하고 영향을 미치기 위한 국제적인 활동을 강화하고, 공격적 사이버를 전력의 수단으로 본다. 사이버 보안은 진정으로 통합된 국가 전략적인 접근을 필요로 한다. 이 전략은 리더십과 합동에 대한 책임을 국무장관들에게 분산시키며, 위임 행정부의 참여를 필요로 한다. 성공 여부는 영국의 강점인 정부 간의 협동적인 노력 위에서 가능하다.

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

51. 범 사회적 노력. 우리의 목표는 전국의 기관에서 의사 결정 하는데에 도움이 되는 국가 전략 접근 방식을 지향하며; 영국 및 전 세계 파트너와 더욱 강력한 협업을 위한 기반을 제공하는 것이다. 이를 현실로 만들기 위해 해야 할 일이 산재한다. 단기적인 조치로는 (i) 새로운 "국가 사이버 자문단" 설립, 민간 및 제3 부문의 고위 지도자 초청, 우리의 접근 방식에 과제, 지원 및 정보 제공, (ii) 대규모, 종종 수도를 기반으로 한 계획부터 지역적으로 제공되는 모델까지 사이버 혁신 프로그램의 방향을 전환, 지역 산업, 혁신가, 법률 집행 기관 및 학계의 파트너십 구축, 그리고 (iii) 사이버 인력의 다양성을 높이기 위한 조치, 전 국민의 기술과 재능을 활용하고 육성할 수 있는 것이 국가 안보에 매우 중요하다는 것을 인식하는 것이다. 이 전략은 북아일랜드, 스코틀랜드, 웨일스의 위임 정부, 산업, 법률 집행 기관, 규제 기관, 학계, 시민 사회 및 국제 파트너와의 협력을 통해 알려졌다. 우리의 목적은 이행 기간 동안 이러한 소통의 장을 열어 두는 것이다.

52. 사이버 공간에 중요한 기술에서 경쟁 우위를 육성하고 보호하기 위한 보다 사전 예방적인 접근 방식. 통합 검토서 (IR) 및 후속 전략은 이미 인공지능, 양자 기술 및 데이터와 같은 영역에서 이러한 접근법을 채택하기 시작했다. 이 전략은 안전한 마이크로프로세서 설계, 운영 기술 및 암호의 보안에 대한 추가적 공약을 포함한다. 운영 기술 보안을 위한 국가 연구소는 업계 및 학계와의 협력을 통해 최고 수준의 사이버 복원력을 구축하는 데 초점을 맞춰 설립되었음을 공표한다. 그리고 맨체스터의 새로운 응용 연구 허브를 포함한 국립 사이버 보안 센터(NCSC)의 connected place(연결 공간)와 교통 등 분야의 신흥 기술을 중점적으로 하는 연구 역량 확대를 발표한다. 이 전략은 새로운 기술에도 안전성을 더하기 위한 접근 방식을 홍보하여 "설계 때부터 안전하게" 만듬으로써 우리의 성공적인 작업의 기반을 마련하도록 한다. 이는 우리가 통신 분야에서 해왔던 것처럼 필요한 곳에 다양하고 안전하며 복원력있는 기술 공급망을 촉진하기 위해 규제와 입법의 수단을 더욱 활용할 것을 의미한다.

53. 정부 주도로 사이버 보안을 촉진하기 위한 핵심 노력을 크게 강화한다. 우리는 정부 사이버 보안의 신속하고 급진적인 점검, 부서에 대한 명확한 기준 수립, 레거시 IT 인프라 문제 해결에 그 어느 때보다 많은 투자를 할 것이다. 사이버 공격에 맞서 정부의 중요한 기능은 2025년까지 크게 강화될 것이며, 2030년까지 공공 부문 전체에 걸쳐 모든 정부 기관들이 이미 알고 있는 취약점과 공격 방법에 탄력적으로 대처할 수 있도록 보장할 것이다. 우리는 국민들로부터 최대한 많은 부담을 덜어주면서 시민들을 보호하고 참여시키기 위해 더 많은 일을 할 것이다. 우리는 디지털 환경을 강화하여 사이버 범죄와 사기로부터 국민들을 보호하고 사이버 보안 기준을 높이기 위해 제조사, 소매 업체, 서비스 제공 업체 및 공공 부문에 더 많은 책임을 부여할 것입니다. 경제 전반에 걸쳐 규제와 인센티브를 부여하고 더 많은 지원을 제공함으로써 사이버 복원력에 대한 민간 부문의 참여와 투자 수준을 끌어올릴 것이다. 우리는 공급망 리스크에 더욱 집중하여, 기관들이 다양한 개입 테스트를 통하여 기관들이 공급자에 의한 사이버 보안 위험에 대응할 수 있도록 도와주고 선례들이 전달이 잘 되도록 할 것이다.

54. 우리의 적들을 방해하고 저지하며 사이버 공간에서 영국의 이익을 보호하고 증진시키기 위한 더 통합되고 지속적인 작전 수행. 이러한 작전은 정부 전반에 걸쳐 외교적, 정책적, 운영적 수단을 폭넓게 활용할 것인데, Lancashire의 Samlesbury에 근거지를 둔 국가 사이버 군(NCF)의 설립과 확장으로 크게 보강이 될 것이다. 우리는 NCF의 능력을 더 일상적으로 활용하여 국가와 비국가 활동가들의 위협을 방해하고 영국의 더 넓은 국가 안보 이익을 지원할 것이다. 또한 우리의 작전은 국가, 지역 및 지방 단위의 법률 집행을 위한 고급 역량에 대한 주요 신규 투자로부터 이점을 취할 것이다. 이것은 랜섬웨어와 더불어 점점 더 혁신적인 사이버 범죄자들로부터 오는 실질적인 위협을 해결하는 데 도움을 줄 것이다. 또한 우리는 영국의 자율적인 사이버 제재 체제와 귀속 절차를 이용하여 우리의 적들에게 비용을 부과하고 악의적이고 무모한 공격에 대해 알릴 것이다.

55. 사이버 파워를 영국의 외교 정책 아젠다의 핵심에 두고 전략의 모든 부분이 국제적인 참여를 필요로 한다는 것을 인식할 것이다. 우리는 디지털 권위주의 확산에 대응하기 위해 핵심 동맹을 강화하고 더 넓은 범위의 국가들과 협력할 것이다. 향후 몇 년 동안, 우리는 협력국을 지원하기 위한 국제 프로그램에 대한 투자를 늘려 그들의 복원력을 구축하고 사이버 위협에 대응할 수 있는 능력을 향상시킬 것이다. 그리고 우리는 국제적 목표를 지원하기 위해 운영 및 전략적 커뮤니케이션 전문 지식, 사고적 리더십, 무역 관계 및 산업 파트너십을 포함한 모든 범위의 국내 강점을 더 잘 활용할 것이다.

영국 전역의 역할 및 책임

56. 사이버에 대한 범사회적 접근 방식은 우리 전략의 중심이다. 우리는 민·관·제3부문 각 부문이 국가적 노력에 중요한 역할을 담당하여 지속적이고 균형잡힌 파트너쉽을 구축해야 한다.

시민

57. 이 전략은 시민들로부터 사이버 보안의 부담을 최대한 덜어주는 것을 목표로 하지만 우리 모두는 계속해서 중요한 역할을 할 것이다. 정부는 사이버 공격이 사람들에게 해를 끼치기 전에 막기 위해 최대한 노력할 것이지만, 일부 위협 활동가들은 이러한 보호를 피할 방법을 찾을 것이다. 우리는 물리적과 가상 세계에서 소중한 자산의 보안을 개선하기 위한 조치를 취할 수 있다.[20] 즉, 우리의 하드웨어(스마트폰 및 기타 기기)뿐만 아니라 우리의 사생활과 직업에서 자유, 유연성 및 편의를 제공하는 데이터, 소프트웨어 및 시스템을 보호하기 위한 모든 합리적인 조치를 취해야 할 개인적 책임이 따른다. 이를 지원하기 위해 정부는 기술적으로 정확하고 시기 적절하며 실행 가능한 조언을 제공한다. 시민 사회 단체와 지역 사회 단체도 사람들이 사이버 위험을 인지하고 보호할 수 있도록 지원하는 중요한 역할을 한다. 예를 들어, 많은 자선 단체들은 취약한 그룹에게 적합한 지원, 조언 및 인식 제고를 제공한다.

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

기업과 기관

58. 기업과 기관은 사이버 위험을 효과적으로 대처하고, 사이버 복원력을 갖추며, 고객과 서비스를 사용하는 사람들을 지원할 책임이 있다. 기업과 기관은 운영, 혁신 및 성장을 위해 디지털 기술과 온라인 서비스에 점점 더 많이 의존하고 있다. 이는 서비스의 질을 높이지만 기업과 기관이 책임지고 있는 개인 데이터 및 디지털 자산의 양이 계속 증가함으로써 새로운 위험과 과제를 발생시킨다. 따라서 서비스를 유지하는 동시에 데이터와 자산을 보호해야 하는 책임이 따른다. 그렇게 하지 않을 경우 기관의 상당한 평판 및 경제적 영향을 미칠 수 있으며 그들의 고객에게 피해를 입힐 수 있다. 필수 서비스 사업자와 주요 디지털 서비스 제공자(예: 클라우드 서비스)는 그들이 직면한 사이버 위험을 해결하고 네트워크 & 정보 시스템 규정('NIS 규정')에 명시된 의무를 이행해야 할 특별한 책임이 있다. NCSC의 조언과 지침은 모든 기업과 기관이 정보, 자산 및 시스템을 보호할 수 있도록 지원하는데 도움이 된다. 또한 정보위원실(ICO)은 영국 일반 데이터 보호 규정에 따른 사이버 보안 의무를 지고있는 기관들에게 영국 일반 데이터 보호 규정에 따른 조언을 제공한다.

사이버 보안 분야 및 주요 기술 기업

59. 영국의 성장하는 사이버 보안 분야는 우리가 직면한 새로운 사이버 위협과 과제에 대응하는 데 중요한 역할을 가지고 있다. 연결 가능한 제품의 급속한 확산과 기업과 기관의 빠른 디지털 변화는 사이버 보안 분야가 성장하고 혁신할 수 있는 기회를 제공하며 새로운 서비스와 제품을 제공하고 있다. 이 전략은 정부가 영국 사이버 보안 분야의 성장을 지속적으로 지원하고, 우리의 파트너십을 유지하고 강화함으로써 이 분야 기업과 기관들의 능력과 전문성을 통해 이익을 얻는 방법을 설명한다. 또한 영국의 기술 전문성과 노하우를 충분히 활용할 수 있도록 학계, 더 넓은 기술 커뮤니티 및 민간 부문 간의 광범위한 파트너십을 강화하고자 한다.

60. 디지털 서비스를 제공하는 주요 기술 기업은 영국의 기업과 기관이 활동할 수 있는 안전한 환경을 보장하는 데 중요한 역할을 한다. 특히 관리형 서비스 제공 업체와 여러 활동을 통합하는 플랫폼 비즈니스의 경우 더욱 그렇다. 기업들은 그들이 제공하는 서비스가 '기본적으로 안전'하며 고객들의 보호 조치에 지나치게 의존 하면 안된다. 주요 기술 기업들도 자체 사이버 복원력을 우선시해야 할 책임이 있다. 클라우드와 온라인 서비스에 대한 기업, 정부 및 더 사회의 의존도가 증가함에 따라 새롭고 특별한 취약점과 상호 의존성이 생겨나고 있다.

정부

61. 영국 정부는 적대자들의 위협에 대응하기 위해 가장 수준 높은 위협의 필요한 정보를 모으고, 법을 만들고, 집행하며, 국가 기준을 설정하고, 공격적 사이버 작전을 실행할 특별한 위치에 있다. 우리는 이 전략을 통해 국가 사이버 역량 강화에 투자할 것이다. 정부 부처와 공공 부문 기관도 자체 네트워크와 시스템을 보호할 책임이 있다. 정부는 중요한 데이터의 소유자이자 서비스 제공자로서 정보 자산에 대한 안전 장치를 제공하기 위해 엄격한 조치를 취한다. 마지막으로, 정부는 또한 국민들, 기업들, 그리고 기관들에게 온라인에서 그들 자신을 보호하기 위해 무엇을 해야 하는지 조언하고 알려야 할 중요한 책임이 있다. 여기에는 중요 기업과 기관들이 우리 모두를 보호하기 위해 기준을 설정하는 것을 포함한다.

62. 사이버 정책의 대부분 영역과 이 전략에서 약술된 대부분의 조치들은 국가 안보, 외교 및 국방, 통신, 제품 표준 및 안전, 소비자 보호와 같은 유보된 사안과 관련이 있다. 그러나 이 전략의 개발 및 실행은 **북아일랜드, 스코틀랜드, 웨일스의 위임된 정부**의 의견, 조치 및 투자에 의존하고 있다. 이는 특히 교육, 치안 및 공공 부문을 포함한 특정 중요 분야의 사이버 복원력과 같이 이 전략의 '생태계' 및 '복원' 요소에 주로 위치하는 위임된 정책 부분에 해당되는 경우에 더욱 관련이 있다. 영국 전역에 최대의 영향을 미치기 위해 영국 4개국에 걸친 조정과 협력은 필수적이다. 이를 위해서는 국무조정실 및 기타 영국 정부 부처가 웨일스, 스코틀랜드, 북아일랜드와 조기에 정기적으로 참여하여 우선 순위와 계획에 대한 정보를 공유해야 한다. 이는 또한 중복을 방지하고 공공 자금에서 최고의 성과를 내는데 도움이 된다. 위임된 정부들은 영국 정부 전략과 연계하여 그들만의 사이버 전략과 계획을 계속 개발할 것이다.

국립 사이버 보안 센터

"영국을 거주하고 온라인에서 일할 수 있는 가장 안전한 곳으로 만들기 위하여"

국가사이버보안센터(NCSC)는 2017년에 국가 통신 본부(GCH)의 일부로서, 사이버 보안 분야의 영국 국가 기관으로 공식적으로 출범했다: 지식 공유, 시스템 취약점 해결 및 주요 국가 사이버 보안 문제에 대한 리더십 제공한다.[21] NCSC의 설립은 정부의 운영 구조를 단순화하고, 국가 수준의 사이버 사고에 대응하는 영국의 능력을 변화시켰으며, 기업과 개인들을 온라인에서 자동적으로 안전하게 만드는 데 도움을 준 혁신적인 디지털 서비스의 출시를 가능하게 했다.

우리는 NCSC가 활동을 뒷받침하는 지속적인 역량과 특성을 명확히 하고, 지속적으로 자금을 지원받고, 지금까지의 운영 경험이 전국적인 범위에서 가능한 최대 영향을 미칠 수 있는 곳에 NCSC역할에 충실하게 함으로써 향후 10년의 과제를 수행하는게 적합하다는 것을 확신하고 있다.

NCSC의 활동을 뒷받침하는 지속적인 역량과 특성은 다음과 같다:

- 영국이 필요로 하는 사이버 보안 분야 및 전문 분야에 대한 세계적 수준의 기술 전문성
- 영국의 국익에 대한 현재 및 잠재적 사이버 위협(의도와 능력)에 대한 비교불가 통찰력
- 전 범위의 영국 국가 안보 역량과 사이버 보안 목표의 권한에의 접근
- 학계, 산업계 및 국제 협력사와 연계하여 사이버 보안 커뮤니티에 직접적 영향
- 전세계적으로 영국 국익의 안전과 보안에 중요한 암호화 기능 및 서비스

새로운 전략 하에서 NCSC의 주요 책임 범위는 다음과 같다:

- 디지털 서비스(예: Active Cyber Defence)를 통해 규모에 맞는 보호를 제공하고, 기술 변화를 주도하며, 국가적으로 중요한 사이버 사고에 대한 대응을 처리하고, 국가 사이버 군(NCF)를 통해 **영국의 사이버 피해를 줄이기 위한 직접적인 조치를 취한다.**

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

- 영국 전역의 국민, 기업 및 기관이 자신을 보호하고 온라인 상의 모든 사람에게 영국을 안전한 곳으로 만들기 위해 사용할 수 있는 맞춤형 전문 지식과 특별한 지식을 제공함으로써 **영국 사회 전체가 스스로를 보호할 수 있도록 지원한다.**

- NCSC의 핵심 역량에서 도출된 권위 있는 기술 도입과 위협 평가를 범 정부에 걸쳐 정책 우위를 제공함으로써 국민, 기관과 이익을 디지털적으로 안전하게 개발하고 도입하는 것을 지원하여 가장 중요한 **사이버 보안 문제에 관한 영국 정부의 정책과 규정에 대한 기술적 견해를 제공한다.**

- NCSC의 National Crypt-Key Centre를 통해 **영국의 자립적 역량을 제공하여,** 가장 유능한 적들의 공격으로부터 영국 군과 국가 안보 커뮤니티가 의존하는 중요 정보들과 서비스를 보호한다.

- 모든 수준의 사이버 교육에 대한 기술적 토대를 제공하고 산업을 참여 및 지원하여 사이버 분야에 대한 투자를 촉진함으로써 **사이버 기술 및 투자 성장을 지원한다.**

NCSC는 또한 영국의 편집자적 독립성을 가진 사이버 평가 기능인 NCSC 평가를 통해 이 국가 사이버 전략의 목표에 기준점을 두고 진행 상황 평가에 기여할 것이다.

국가 사이버 군

2020년에 설립된 국가 사이버 군(NCF)은 영국이나 동맹국에 해를 끼치는 자들에게 대항, 방해, 저하, 경쟁하기 위해 사이버 공간을 통해 활동할 책임이 있으며, 국가를 안전하게 하고 국내외에서 영국의 이익을 증진시킬 책임이 있다. NCF는 국방과 정보기관의 대략적으로 동등한 비율로 구성되어 있으며, 그들의 전문지식, 자원, 권한을 하나의 지휘구조로 통합한다. 본부는 Lancashire의 Samlesbury에 있다.

국가사이버 군은 국방 지원과 같은 국가 안보, 영국의 경제적 웰빙, 국가 지원 범죄자 및 비국가 지원 범죄자들의 심각한 범죄 활동의 방지 등과 같은 국익에의 광범위한 성과를 이루어 내는 조직이다. 사이버 군의 업무는 아래 3가지 범주로 분류된다.

- 국경을 넘어 인터넷을 사용해 영국과 다른 민주주의 사회에 피해를 주려하는 테러리스트, 범죄 조직 및 국가의 위협에 대응

- 사이버 공간에서 데이터 및 서비스의 기밀성, 진실성 및 가용성을 방해하는 위협에 대응(즉, 사이버 보안 지원)

- 영국 국방 작전에 기여하고 영국의 외교 정책 아젠다의 이행을 지원(예: 민간인을 보호하기 위한 인도주의적 위기에 개입)

NCF 작전은 개인과 그룹에 영향을 미치고 온라인 및 통신 시스템을 방해하며 물리적 시스템의 작동을 저하시키는 데 사용될 수 있다. 이러한 유형의 활동을 공격적 사이버(OC)라고 한다.

NCF 작전은 1994년 정보법, 2016년 수사권법이 포함된 잘 확립된 법적 틀에 따라 진행된다. 영국은 이전에도 NCF는 무력 분쟁법을 포함한 국제법에 따라 능력을 개발하고 배치한다는 점을 분명히 한 바 있다. 이 활동들은 장관 승인, 사법 감독, 의회 검토의 대상이 되어, 사이버 활동을 위한 영국의 통치 체제는 세계에서 가장 강력한 국가 중 하나가 되었다.

영국은 정기적으로 개별 사이버 작전에 대해 이야기하지는 않겠지만 NCF가 수행할 수 있는 작전 활동의 종류는 다음과 같다:

- 테러 집단의 지휘 통제 통신을 무력화하고 극단주의 미디어 확산을 제한함으로써 그들의 계획을 실행하는 것을 막는다.
- 상대 무기 시스템을 저하시켜 영국 군에 해를 끼칠 위험 감소
- 민주주의와 자유, 공정, 공개 선거를 보호하기 위해 이를 방해하는 조직적인 국가 허위 정보 캠페인에 대응
- 범죄 집단의 온라인 플랫폼 및 서비스 사용을 방해하여 그들의 활동으로부터 이익을 얻는 것을 방지
- 국제 제재를 피하려는 상대의 노력을 방해함으로써 국제 제재를 집행하는 것을 돕는다.
- 국가 기반 시설을 교란하려는 적국의 사이버 공격으로부터 영국과 다른 국가를 보호한다.
- 중요한 정보에 대한 접근 능력을 보호하여 인도주의적 위기에 처한 민간인을 보호한다.

사이버 공간에서 그리고 사이버 공간을 통한 효과적 활동의 국가 최고 기관으로서 NCF는 다른 국가와 함께 영국의 능력을 개발하고, 통합하고, 활용하여 최대의 효과를 성취하도록 한다.

사법 시행 기관의 국가 사이버 범죄 네트워크

국가 사이버 보안 전략 2016-2021의 과정에 걸쳐 설립된 사법 기관의 국가 사이버 범죄 네트워크는 개인, 기관 또는 전 분야에 대한 모든 형태의 사이버 공격에 대해 정보 주도의 대응을 제공할 수 있는 완전히 통합된 사이버 범죄 대응을 개발했다. 이것은 국가, 지역 및 지방 수준에서 운영되는 전국적인 시스템이다. 이는 피해자 지원을 제공하고 기업과 사람이 보호받고 신속하게 회복할 수 있도록 도우며 가해자에 대한 형사 사법 결과를 추구한다.

국립범죄청(NCA)의 국가 사이버 범죄 부서 (NCCU)는 스코틀랜드 경찰과 북부 아일랜드 경찰과 런던 경찰국의 사이버 범죄 부서와 제휴하여 잉글랜드와 웨일스의 9개 경찰 지역의 지역 **사이버 범죄 부서 (RCCU)** 네트워크의 지원을 받아 국가적 지도력과 협동적 대응을 제공한다.

이들은 43개 경찰력에 각각 소속되어 있고 지역 코디네이터를 통해 같이 움직이게 되어 있는 현지 **사이버 범죄 부서(LCCU)**에 의해 더욱 보완된다. 이러한 지방 및 현지 사이버 범죄 부서는 범죄자를 조사 및 추적하고, 기업과 피해자를 공격으로부터 보호하고, 취약한 개인이 사이버 범죄에 당하는 것을 방지하기 위해 파트너와 협력한다.

중앙화한 범죄 보고, 분류, 분석은 **런던시 경찰청(City of London Police)**가 주관하는 **Action Fraud**를 통해 제공된다. 가장 심각하거나 복잡한 사례들은 국가 경찰청(NCA)와 지방 네트워크로 이첩되어 추가 조사를 하게 되며, 기타 사건은 지역 경찰서에게 전달된다. 또한 런던 시 경찰청은 경제 범죄 피해자 지원팀을 포함한 피해자 지원을 조율하기도 한다.

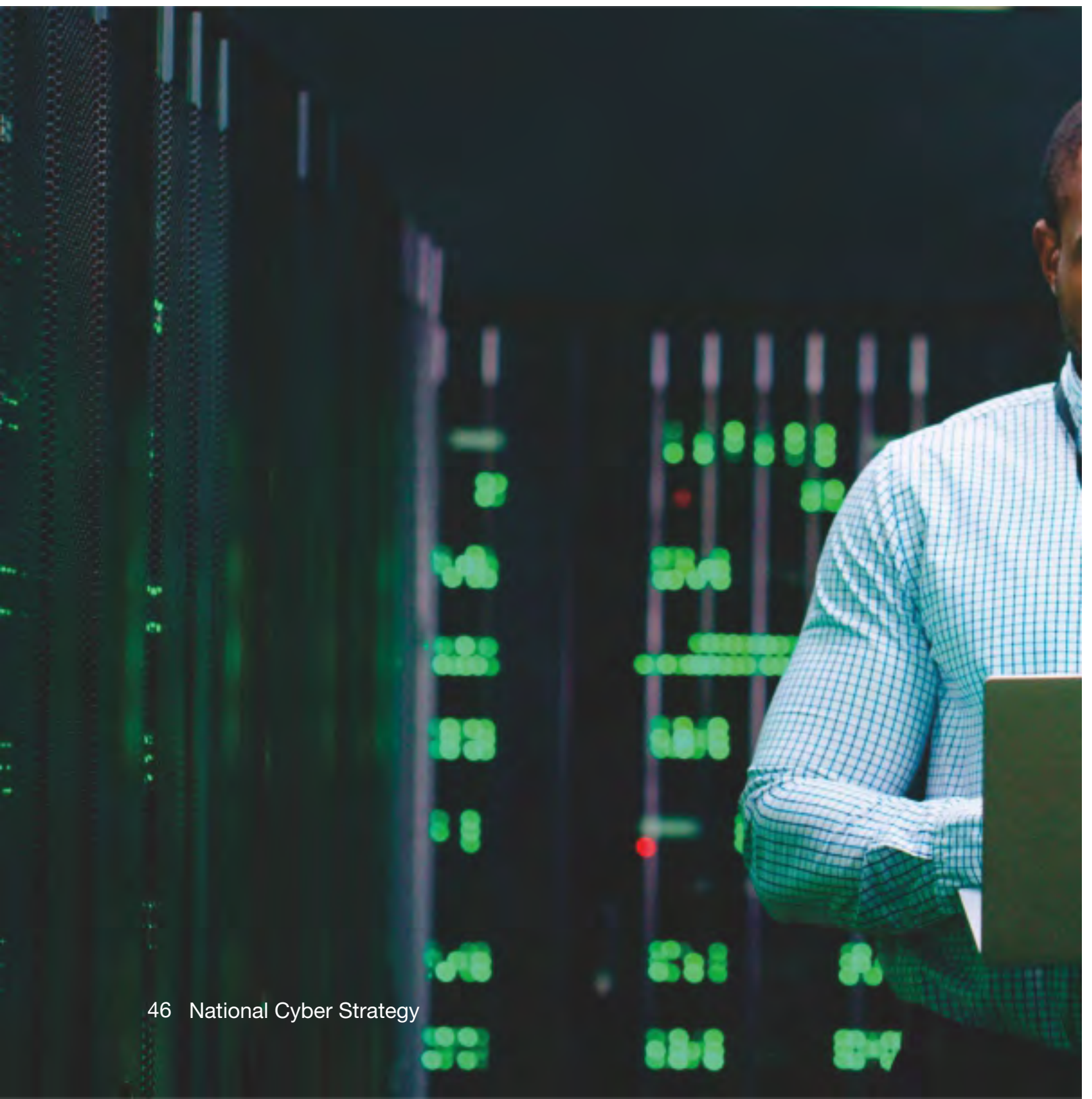
변화된 범죄 과학 수사, 정보 및 데이터의 공유 능력과 시스템을 통합하여 국가 차원 및 지방 조직이 모든 전문 최고 역량과 개발되고 있는 기법에 접근 가능한 통합 플랫폼을 만들고 있다. 여기에는 보안 및 정보 커뮤니티의 파트너와 효과적으로 협업할 수 있는 기능, 특히 혼재된 범죄좌와 국가 단위 위협에 대응할 수 있는 기능이 포함 한다. '한 번 구축할때, 전 사이버 범죄 네트워크의 이익을 위해 국가적으로 구축 할 것'이라는 신조와

함께 이러한 기능들은 현지 사이버 범죄 수사대에게로 지방 협업 기관을 통해 전달된다. 이러한 범 시스템 접근 방식은 이미 사이버 범죄 위협에 대한 상당히 향상된 대응을 제공하고 있다.

사이버 범죄 네트워크 법 집행 기관은 국제·국가·지역·지역 차원의 위협을 주는 활동가들의 사이버 공간 내의 악의적인 활동에도 응용 범죄학적 대응을 지속 할 것이다. 이러한 대응은 다음과 같은 무력화 방법으로 보완 될 것입니다:

- 전문적인 고급 수사 및 무력화 사이버 역량 개발
- NCA의 광범위한 국제 네트워크를 활용하여 정보 및 증거를 바탕으로 협력국 개입 지원
- 범죄 조직의 범죄 시장 이용 저지와 서비스를 활성화를 통해 그들의 활동으로부터 얻는 이익을 사전 방지
- 사이버 범죄에 이용되는 기반 시설을 분해 및 무력화하여 영국 및 기타 국가를 사이버 범죄로부터 보호
- 고위급 위반자에 대한 제재 활동 및 범죄 행위 공개에 기여
- 사이버 범죄의 수익으로부터 암호 화폐 및 기타 자산 압류

Part 2:
실행



전략 축 1:

영국 사이버 생태계

영국의 사이버 생태계 강화

63. 이 전략이 성공하기 위해서는 영국이 알맞은 인력, 지식, 파트너십을 갖출 수 있도록 해야 한다. 우리는 다양하고 기술적으로 숙련된 인력, 활발한 연구 커뮤니티, 국제적으로 경쟁력 있는 사이버 부문 및 정부, 산업 및 학계 간의 강력한 협력을 기반으로 하는 중요한 기술을 선도할 수 있는 번영하는 지역 혁신 생태계를 갖춰야 한다.

64. 사이버 생태계의 성장은 정부의 개입에 의존하지 않고 자립적일 필요가 있다. 이 전략의 과정에 걸쳐 우리는 대체로 중앙에서 관리되는 맞춤형 기술 및 혁신 프로그램이 아니라 보다 지속 가능하고 체계적이며 지역적인 접근 방식에서 재정 지원을 받는 것으로 전환할 것이다. 우리는 더 많은 사람들이 사이버 관련 직종에 종사하는데 필요한 기술을 습득하도록 지원하고 영감을 주기 위해 기술과 교육 시스템에 대한 정부의 광범위한 개혁을 구축할 것이다. 그리고 우리는 사이버 인력의 다양성을 증가시키기 위해 다양한 구체적인 행동을 우선 순위에 둘 것입니다. 이것은 모든 사람들이 이러한 직종에 종사할 수 있도록 하는 것뿐만 아니라 우리가 전체 국민의 재능과 기술을 활용하여 국가 안보에 중요한 임무 수행을 위해서이다. 우리는 또한 사이버 부문 성장이 사이버 부문 고용의 45%로 추산되고 외부 투자의 85%를 차지하는 런던과 남동부뿐만 아니라 영국 전체에 이익이 되도록 할 것이다.[22]

65. 전반적으로 우리는 업계 리더, 학계, 혁신가, 법 집행 기관, 국가 안보 공동체 및 사이버 위협에 대한 영국의 복원력을 높이기 위해 협력하고자 하는 사람들의 협력을 촉진하는 보다 전략적인 역할을 맡게 될 것이다. 우리는 학교에서 사이버 교육을 받는 방법에서부터 경제 규제 기준을 높이는 방법에 이르기까지 사이버 생태계를 지원하기 위해 정부의 모든 수단을 동원하여 영국이 미래의 위협으로부터 스스로를 보호하는 데 필요한 필수 역량을 키우도록 할 것이다.

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

목표 1:
사이버에 대한 사회 전체의 접근 방식을 지원하는 데 필요한 구조, 파트너십 및 네트워크 강화

66. 사이버 전력은 사회 전체의 접근을 필요로 한다. 우리의 경쟁적 우위는 영국 전역에서 인재를 육성하고 활용하며, 공공 부문, 산업 및 학계 전반에 걸쳐 적합한 인력이 협력하게 함으로써 사이버 커뮤니티 전체를 통합하는 능력에서 비롯된다. 우리는 산업계와 진정한 통합 공급 파트너십을 형성하고 영국의 국가 및 지역에 걸쳐 광범위한 접근을 위해 북아일랜드, 스코틀랜드 및 웨일스의 위임된 정부와 긴밀히 협력한다. **우리는 2025년까지 다음과 같은 성과를 달성할 것이다.**

67. 새로운 국가 사이버 자문단을 설립하고 사이버 보안 연구 및 교육을 위한사이버 성장 및 복원 파트너십 네트워크 및 우수 학술 센터를 구축함으로써 산업, 학계 및 국민과의 **보다 포괄적이고 전략적인 국가 사이버 대화**를 만들어 낸다.

68. 부문별 성장과 비즈니스 복원력을 위한 **영국 전역의 보다 통합되고 효과적인 지역 사이버 네트워크를 통해 정부,** 기업 및 학계 간의 강력한 파트너십을 실현한다. 우리는 지역 사이버 모임과 최근 설립된 영국 사이버 클러스터 협업(UKC3), 증가하는 지역 사이버 혁신 센터 및 사이버 복원 센터와 협력하여 지역 기업, 우수 학술 센터 및 법 집행 기관 간의 연계를 강화할 것이다.

69. 이러한 과정은 국가 사이버 안보 센터(NCSC)와 관계자들, 정부 부처와 외부 기관 및 CNI 및 규제 기관을 포함한 대표하는 경제 부문, 업계, 디지털 및 기술 부문에서 정부와의 더 넓은 대화를 기반으로 이루어 진다.

Ciara Mitchell, Head of Cyber at ScotlandIS

Ciara는 스코틀랜드 사이버 클러스터의 매니저이자 UKC3의 이사회 멤버이기도 하다.

"스코틀랜드의 사이버 클러스터는 스코틀랜드의 사이버 보안 커뮤니티를 지원하는데 핵심적인 역할을 하고 있다. 스코틀랜드에는 클러스터 관리에 대한 전문성에 대한 이해와 번창하는 사이버 분야를 구축할 수 있는 기회가 증가하고 있다. 나는 클러스터의 가치에 대한 인식이 높아지는 가운데 생태계 개발 선도자로서 새로운 영국 사이버 클러스터 협업의 핵심 역할을 맡게 되어 기쁘다. UKC3를 통해 영국의 사이버 보안 분야를 성장시킬 수 있는 플랫폼을 제공하는 협업, 혁신 및 기술 개발에 중점적으로 노력할 것이다."

사이버 기관 (지역 대표)

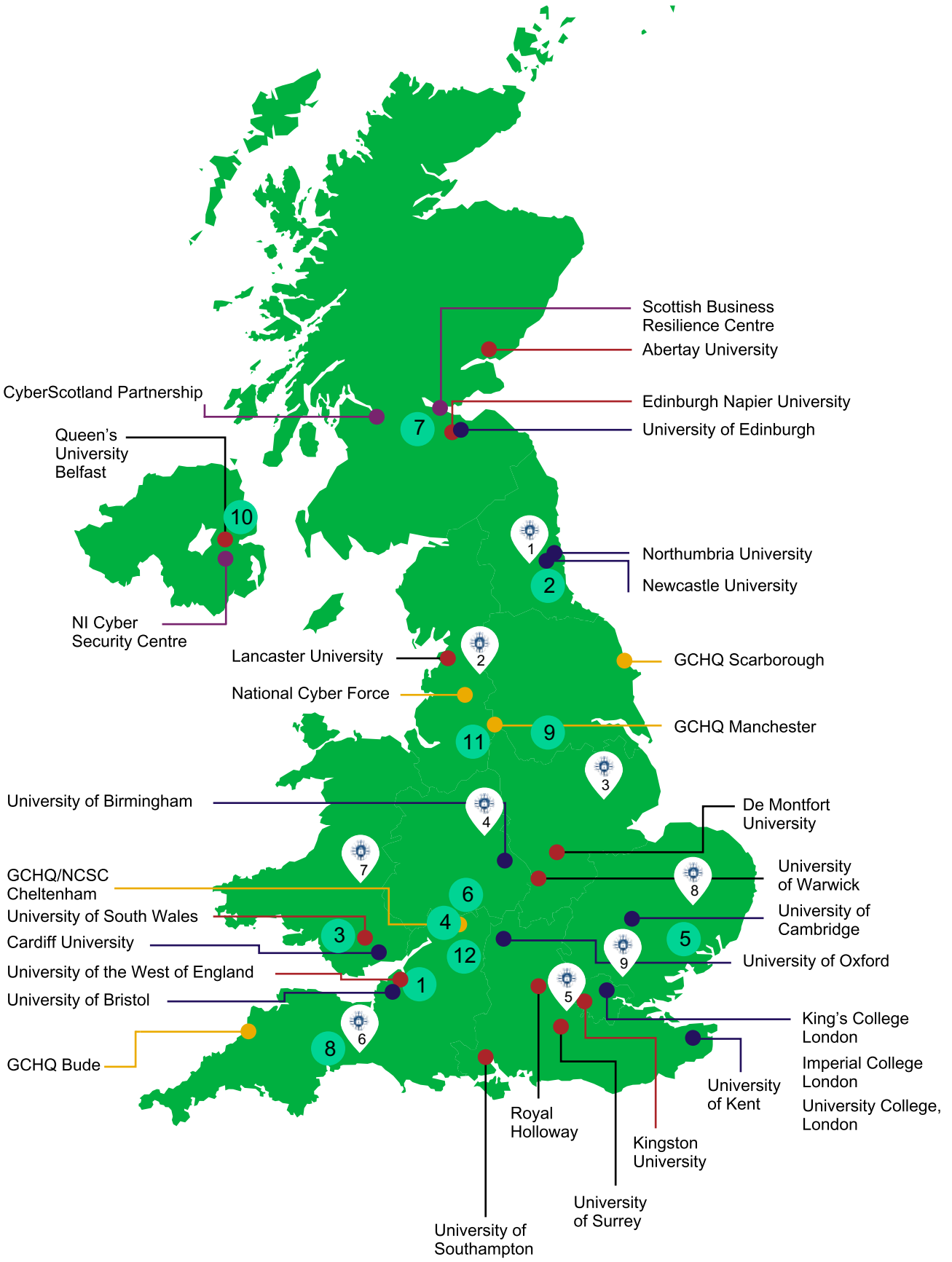
영국 사이버 클러스터

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

- Academic Centre of Excellence in Cyber Security Education
- Change Academic Centre of Excellence in Cyber Security Research*
- GCHQ / NCSC site
- Devolved Authority Organisations

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

1. The Business Resilience Centre for the North East
2. The North West Cyber Resilience Centre
3. The Cyber Resilience Centre for the East Midlands
4. The Cyber Resilience Centre for the West Midlands
5. The Cyber Resilience Centre for the South East
6. The South West Cyber Resilience Centre
7. The Cyber Resilience Centre for Wales
8. The Eastern Cyber Resilience Centre
9. The Cyber Resilience Centre for London


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

목표 2:
미래 인재에 영감을 주고 양성하는 세계적 수준의 사이버 보안 전문직 등을 포함한 다양한 층의 국가 사이버 인력 향상 및 확대

70. 영국의 야심찬 계획의 중심에는 디지털 경제의 핵심 요소를 확보하고 새로운 접근 방식을 혁신하고 개발할 수 있는 지속적이고 다양한 고급 인력을 사이버 인력으로 개발하는 것이 있다. 이는 공공부문 전반에 걸친 전문 지식을 인지 및 유지하고 국가사이버군(NCF)을 포함한 법 집행, 국방, 보안에 대한 역량을 향상시킴으로써 모범적으로 선도하려는 우리의 목표를 뒷받침할 것이다. 이 전략의 다른 부분들과 마찬가지로, 우리는 스코틀랜드, 웨일스 및 북아일랜드의 위임된 정부들과 협력하여 교육 및 기술과 같은 위임된 문제에 대한 영국 정부 계획에 대해 일관된 접근법을 취할 수 있도록 할 것이다. **우리는 2025년까지 다음과 같은 성과를 달성할 것이다.**

71. 교육 및 기술 정책이 국민과 고용주의 요구를 충족하도록 보장하기 위해 영국 4개 국가 전체에 걸쳐 이루어지는 작업을 기반으로 사이버 인력으로 진입하는 데 필요한 기술을 가진 사람들의 수가 크게 늘림. 우리는 사이버 인력에 부합하는 16세 이후 교육 프로그램 확대, 사이버 보안에 대한 다양한 기술 훈련소 자금 지원, 국가 기술 연구소 프로그램의 설립 및 학부생들을 위한 사이버 퍼스트 장학금 제도 지속을 포함한 여러 조치를 통해 이를 수행할 것이다. 이는 정부가 16세 이후 교육과 훈련의 대부분을 2030년까지 강화된 고용주 기준에 맞추려는 작업에 기반을 두고 있다. 이러한 계획은 더 넓은 사이버 커뮤니티를 위해 영국 사이버 보안 위원회와 함께 개발될 것이며 수습 연수, T 레벨 (영국 기술 과목 자격 시험) 및 새로운 고급 기술 자격 요건 등을 뒷받침할 것이다. 이것은 고용주가 자격 요건과 훈련을 설계하고 개발하는 데 중심적인 역할을 할 수 있도록 보장할 것이다.

72. 더 수준 높고, 확고한, 인정받는, 구조화된 사이버 보안 전문직 창출. 영국 사이버 보안 위원회는 영국 왕실 헌장의 지원을 받아 세계 최고의 사이버 보안 지식 기관(CyBOK)을 기반으로 한 전문적인 표준과 사이버 인력으로의 양성 과정을 수립할 예정이다. 또한 사이버 인력 전반에서 우수성과 전문성이 명확하고 일관될 수 있도록 이러한 기준을 전문직에 적용시키기 위해 법률을 포함한 모든 정부 수단을 모색할 것이다.

73. 영국 전역의 대표되지 못한 집단과 취약 계층 커뮤니티에게 사이버 분야 진출하고 번창할 수 있도록 효과적인 지원을 제공함으로써 더욱 **다양한 사이버 인력의 확보.** 우리의 조치에는 더 많은 여성이 사이버 인력에 진출하도록 지원하는 것과 대표되지 못한 집단이 고급 수준으로 발전할 수 있도록 지원하는 구체적인 계획이 포함될 것이다. 사이버퍼스트 걸스 콘테스트를 포함한 우리의 대표 사이버퍼스트 프로그램을 통해 제공하는 비교과 활동의 성공적 운영을 기반으로 실행할 것이다. 우리는 또한 국가범죄청의 사이버 초이스 프로그램을 통해 어려움에 처한 젊은이들을 위한 교육과 진로 접근 기회를 늘려 불법 사이버 활동에서 벗어나 그들의 재능과 열정을 활용할 수 있는 더 긍정적인 기회로 그들을 인도 할 것이다.

74. 우리의 교육 시스템을 통한 안정되고 다양한 고급 인력의 유입. 스코틀랜드에서 컴퓨터 과학 GCSE 및 동등한 자격을 취득하는 지원자들의 활용과 다양성의 증가, 영국의 T Levels, 수습직 및 고등 교육 기회와 같은 더 많은 젊은이들이 교육을 통해 기술 진로를 따를 수 있도록 영감을 주고 지원할 것이다. 그리고 우리는 국립 컴퓨팅 교육 센터(NCE)를 통해 교사들의 기술을 개발하여 그들의 자원과 개발 기회를 제공하여 학생들에게 더 많은 관심을 불러일으킬 수 있도록 할 것이다.

75. 정부는 필요한 사이버 전문가를 더 잘 찾아내고, 모집, 교육 및 유지할 수 있도록 한다. 정부는 사이버 전문가, 정부 및 공공 부문의 고용주로서 본보기를 보여야 하며, 위에서 설명한 조치를 지지하고 그것을 기반으로 발전시켜야 한다. 공공부문 전반에 걸쳐 보다 일관성 있고 효과적인 접근을 하는 한편 공무원이나 고위 지도자를 양성할 수 있는 구체적인 방안을 가다듬고 NCF, NCSC, 법 집행 등 국방 안보 분야에서 역량을 키울 것이다. 여기에는 사이버 속성 과정을 확장하고 더 많은 사이버 보안 견습 프로그램을 제공함으로써 초기 인재를 위한 투자, 대학원 및 인턴, 맞춤형 신경 다양성 프로그램 및 여름 다양성 프로그램을 포함한 NCA 내의 전문 기술 프로그램 지원 등이 포함될 것이다. 그것은 학계, 산업 및 국제적 파트너들과 협력하면서, 방어적이고 공격적인 사이버 훈련을 광범위하게 제공하여 국방 사이버 아카데미로 확장함으로써 국방 사이버 학교의 성공을 주도할 것이다.

영국 사이버 보안 의회

영국 사이버 보안 의회는 사이버 보안 분야에서 세계 최초로 2021년 3월 출범했다. 의회의 임무는 사이버 인력 및 분야 전반에 걸쳐 존재하는 자격 요건, 자격증 및 학위에 명확성과 구조를 제공하는 이 전문 직종의 대변자가 되는 것이다. 의회를 설립으로 사이버 전문직이 의학 및 법률과 기존 직업과 유사하게 경제 전반에 걸쳐 광범위한 기술 및 비기술 전문 지식과 전문성을 통합하고 있다는 것을 인지하게 되는 중요한 단계를 밟게 된 것이다.

의회는 네 가지 목표를 가지고 있다:

- 사고 방식 리더십 및 직업적 기준 설정: 사이버 보안을 정의하는 기준을 개발하고 합의하는 작업을 주도
- 경력과 훈련 : 고용주와 개인이 경력 결정을 내리는데 필요한 조언을 통해 지원한다. 사이버 안보 기술, 직업 개발과 인정 등에 대한 조언 제공
- 직업 윤리: 실무 전문가 및 기관이 사이버 보안에서 윤리 실천을 입증할 수 있는 가이드 라인 원칙 제공
- 다양성 및 포용성: 사이버 보안을 모든 연령과 배경의 사람들에게 직업 기회로서 촉진하고, 분야 내에서 진입과 진출의 장벽을 제거하기 위해 노력

의회는 전문 기관으로서 이 전략의 적용 기간 전체에 걸쳐 신뢰성과 지속 가능성을 성장시키고 확립하기 위해 노력할 것이다.

여왕은 2021년 11월 영국 사이버 보안 의회에 왕실 헌장을 수여하는 것을 승인했다. 이는 최초로 사이버 보안 분야에만 주어지는 표창이며, 해당 분야에 존재하는 다양한 전문 분야를 포괄한다.

우리는 정부, 국방 및 법률 집행을 포함하여 사이버 생태계 전반에 걸쳐 직업 기준과 계획을 실행하기 위해 더 많은 작업을 수행해야 한다는 것을 인지하고 있다. 의회는 청년들과 경력 변경자들이 사이버 분야에서 직업을 찾아볼 수 있도록 지원하는 주요 역할을 할 것이다.

Simon Hepburn, CEO, UK Cyber Security Council
영국 사이버 안보 의회 의장

나의 직무는 영국 사이버 보안 의회를 "사이버 보안 전문가를 위한 대변자"로 홍보하는 것이다. 본 의회는 영국의 사이버 보안 전문가에 대한 자율 규제 기관이며, 우리는 업계가 통합하여 영국이 거주하고 온라인에서 일하기 가장 안전한 곳으로 만들기 위해 국가가 인정하는 기준을 개발, 촉진 및 관리하는 것을 목표로 한다. 의회는 성공적인 결성 계획을 거쳐 2021년 3월 공식 출범했으며, 현재 회원 신청이 가능하다. 이번 국가 사이버 보안 전략은 의회와 함께 개인과 기관이 전문성을 향상시키는 방식으로 일할 수 있도록 보장하는 중요한 요소가 될 것이다.

목표 3:
지속 가능하고 혁신적이며 국제적으로 경쟁력이 있는 사이버 및 정보 보안 부문의 성장을 촉진하여 정부와 경제 전반의 요구를 충족하는 양질의 제품과 서비스를 제공한다.

76. 우리의 국가 사이버 파워를 향상시키고 디지털 성장과 수출을 촉진시키기 위해 영국은 신빙성 있고 최고 기업으로 구성된 강력한 사이버 부문이 필요하다. 영국 기업들은 영국과 전 세계의 산업계와 정부에게 세계 최고의 기술, 교육 및 조언을 제공하고 있다. 그러나 몇몇 기업들은 최첨단 기술을 개발하여 성공 가능한 제품을 제공할 수 있는 단계에 도달하기 위한 지원과 투자에의 연결이 필요하다.

77. 기업들은 또한 다른 기관들도 따르고 있는 정부 승인 기준에 맞춰 혁신하고 있다는 확신을 가질 필요가 있다. 또한 우리는 구매자가 다양한 품질의 광범위한 제품과 서비스로 구성된 복잡한 환경 속에서 필요한 제품을 찾을 수 있게 노력해야 한다. 이것은 결국 생태계 속에서 수요를 촉발하고 더 많은 성장이 가능하게 할 것이다. **우리는 2025년까지 다음과 같은 성과를 달성할 것이다:**

78. 무역과 사이버 수출을 포함한 전 세계 성장의 평균 이상을 달성한 사이버 분야. 영국 내 세계 최고의 대표 사이버 이벤트를 지원하고 우리의 가장 혁신적인 사이버 기업을 무역 사절단 및 국제 사이버 박람회 참여할 수 있도록 초대하여 국내외 사이버 기업들이 새로운 시장에 접근 할 수 있도록 지원할 예정이다. 그리고 공공부문 조달을 보다 효과적으로 활용하고 NCSC 공인 사업자 목록 책자를 발행하여 고급 사이버 보안 제품과 서비스에 대한 수요를 촉진할 것이다.

79. 보다 더 혁신적인 사이버 분야의 구축. 사이버 분야는 초기 단계의 투자가 증가하고 새로 설립하고 성장 가능한 사이버 기업의 증가를 목도하고 있다. 새로 운영 시작한 사이버 런웨이 프로그램으로 기업에게 지원과 Tech National Cyber Programme, Cyber 101, Hut Zero와 같은 과거 프로그램을 통해 얻은 교훈을 제공할 수 있는 유일 담당 부서를 제공하고 있다. 사이버 촉진 역할을 담당하는 NCSC 스타트업을 포함한 Cheltenham 혁신 센터를 진정한 혁신의 국제적 센터인 국가 사이버 혁신 센터로 탈바꿈 시킬 것이다. 우리는 국가 보안 기술 및 혁신 교류 등 공동 창출을 촉진하고 활성화하기 위해 존재하는 조직의 전문 지식을 활용할 것이다. 그리고 영국 비즈니스 뱅크와 국가 안보 전략 투자 펀드와의 파트너쉽을 통해 초기 단계 사이버 창업에 고위험 투자를 장려할 것이다.

80. 동남부 이외의 지역에서 성장이 증가하여 크게 상향 발전한 영국의 사이버 경제 덕분에 코로나바이러스 (COVID-19) 대유행으로부터 회복하고 광범위한 지역 경제 활동의 지원이 가능하게 되었다. 우리는 영국 북서부 샘즈버리에 NCF의 상설 본부를 설립하여 런던 외곽의 기술, 디지털 및 국방 분야의 성장을 촉진하고 지역에서 새로운 파트너십을 창출하도록 도울 것이다. 우리는 런던 외곽과 동남부 지역의 혁신가들과 기업인들이 제품과 서비스를 개발하고 사업을 성장시키며 숙련된 인력을 채용할 수 있도록 지원을 늘릴 것이다. 여기에는 사이버 관련 기술 사업의 성장을 지원하기 위해 설립된 첼트넘 구의회가 이끄는 골든 밸리 캠퍼스가 포함된다. 그리고 지역 사이버 클러스터와의 교류를 통해 영국 내 더 많은 지역에 걸쳐 사이버 기업의 수출 역량을 높이고, 해외 바이어들에게 더 많은 사이버 산업 인재를 선보일 수 있는 이벤트도 준비할 것이다.

81. 독자적으로 입증 가능한 품질 기준을 충족하는 사이버 안보 기술과 상품과 서비스 제공이 가능한 기업의 수가 증가하여 사용자의 만족도를 높임. NCSC 브랜드와 전문성을 활용해 영국 소비자들이 안심하고 서비스를 구매하고 보안을 개선하며 국가 사이버 보안 장벽을 높이도록 조력하여 신뢰할 수 있는 시장을 구축해 2021년 9월 NCSC가 발간한 'NCSC 기술 보증의 미래' 백서와 맥을 같이 하도록 추진할 것이다.[23]

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

Berta Pappenheim, CEO and founder, Cyberfish Company
사이버 휘시 사 대표

사이버피쉬사는 정부의 사이버 강화 프로그램에 참여했다. 우리의 목표는 기업과 정부 팀이 사이버 사고와 같은 업무 중단을 더 잘 처리할 수 있도록 준비하도록 돕는 것이다. 우리는 그들과 함께 사고 시뮬레이션 연습을 실행하고, 스트레스 받고 있는 팀내 역동성을 관찰하고, 개선 방법을 코칭함으로써 이를 수행한다. 대부분의 자문가들은 고문들은 사고 대응의 기술적 측면이나 리더십과 의사 결정의 행동적 측면 중 하나에 능숙하지만 우리 회사는 양쪽의 전문적인 지식을 가지고 함께 이 두 가지에 다 조언을 제공한다. 우리의 활동으로 전 세계 필수 임무 수행 팀에서 일하는 500여 명의 업계 리더들이 관점을 전환하고 팀워크를 개선하여 위기 대응 및 의사 결정을 개선하는 데 도움이 되었다.

사이버 직종에 관심이 있거나 개인 사업을 시작하는 데 관심이 있으십니까?

82. 우리의 이전 전략은 영국에서 사이버 기술 기반과 사이버 보안 서비스 분야를 성장시키는 데 큰 중점을 두었다. 전략적 맥락에서 요약된 바와 같이, 우리는 관련 부문과 수출을 성장시키는 데 있어 상당한 진전을 이루었다.

사이버 기업이 국제 시장을 찾을 수 있도록 지원했다. 영국은 2020년에 42억 파운드의 사이버 서비스를 수출했다.

온라인 사이버 포털인 사이버 교류 (Cyber Exchange)를 통해 영국 전 지역의 사이버 기업들을 한데 모은다.

사이버 성장 파트너십은 성장의 장벽을 깨기 위해 정부와 업계를 하나로 모았다.

83. 우리는 지난 5년간 영국의 사이버 생태계가 번창할 수 있도록 혁신가들이 사업을 성장 및 확장할 수 있도록 지원해 왔다:

NCSC for Startups는 160개가 넘는 새로운 기업 시험에 이미 참여한 가운데 혁신가에게 가장 중요한 전략적 도전이 어디에 있는지를 가르키고 있습니다.

LORCA는 72명의 사이버 혁신가들이 2억 파운드 이상의 투자를 유치하고 3,700만 파운드 이상의 수익을 올릴 수 있도록 도왔다.

Cyber Runway는 혁신가들이 Hutzero와 Cyber101의 성공을 기반으로 사업을 시작, 성장 및 확장할 수 있도록 지원한다.

84. 우리는 사이버 인력에 진입하는 연간 10,000명의 전문인력의 부족을 줄이기 위해 노력해 왔다:[24]

사이버 퍼스트 장학금 제도는 대학생들을 지원하고 있으며, 매년 수백 명의 실무 경험이 있는 사람들을 사이버 인력으로 보내고 있다.

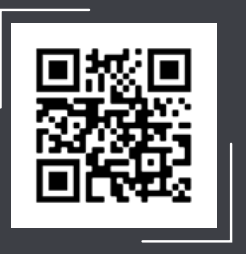
현재 교육부의 '직업을 위한 강좌' 제도를 통해 제공되는 초기 학습 성과를 위한 세 가지 사이버 제안과 업계에서 설계한 네 가지 사이버 수습 기준이 존재한다.

최근 국가 기술 기금을 통해 지원되는 사이버 훈련소는 9곳이며, 사람들을 흥미로운 사이버 직종으로 인도하고 더 많은 사이버 캠프가 매 회계 연도에 계획되어 있다.

85. 우리는 사이버 인력을 전문화하여 기관이 필요한 기술을 보다 쉽게 파악하고 개인이 알아야 할 내용을 쉽게 탐색할 수 있도록 지원하고 있다.

영국 사이버 보안 의회는 사이버 보안에 관한 세계 최초의 전문 기관이다. 기존 전문 기구가 지금까지 해온 모든 업무를 바탕으로 명확하고 일관된 전문 기준을 세우기 시작했다. 의회는 현존하는 무수한 자격 요건 중에서 효과적인 자격 요건이 무엇인지를 명확하게 찾아 낼 것이다.

사이버보안지식단(CyBOK)은 사이버 보안 분야에 대한 교육과 전문 교육을 알리고 지원한다.



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

우리는 16%만이 여성이고 고위직의 3%만이 여성 및 소수 민족인 분야의 불평등을 해결하면서 모두가 사이버 노동력에 참여할 수 있도록 노력해 왔다.[25]

사이버퍼스트 과정과 디스커버리 프로그램은 지난 5년 동안 거의 30만 명의 11-17세 청소년들을 참여시켰다.

영국 사이버 클러스터 협력은 지역 전체에 걸쳐 기회와 전문 지식을 이용할 수 있도록 업계, 학교 및 대학 간의 파트너십을 구축하고 있다.

NCA의 사이버 초이스 프로그램으로 젊은이들이 정보에 입각한 선택을 하고 그들의 사이버 기술을 합법적으로 사용할 수 있도록 돕고 있으며, 인식을 높이고 수습 제도나 현장 실습과 같은 더 나은 대안을 제공하고 있다.

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

전략 축 2:
사이버 복원력

복원력 갖춘 번영하는 디지털 영국의 구축

87. 사이버 보안과 복원력은 사이버 강국으로서 우리의 더 넓은 전략적 목표의 기초가 된다. 사이버 보안과 복원력 없이는 우리는 더 나은, 더 공정하고 강력한 디지털 기술의 전환적 잠재력을 충분히 활용하여 사이버 공간에서 그리고 사이버 공간을 통해 영국의 전략적 우위를 보호할 수 없다. 우리는 강력한 사이버 국방을 구축하여 국가, 지역 및 개인 차원에서 영국의 디지털 네트워크, 정보 및 자산을 보호하고 사건 발생 시 복원력을 보장하기 위한 조치를 취해야 한다.

88. 그리고 이 장에서는 사이버 복원력을 집중적으로 설명하겠지만, 더 효과적이기 위해 영국의 복원력을 증진시키기 위한 총체적이고 사회 전체의 노력을 필요로 한다는 점을 강조한다. 통합 검토서(IR)의 핵심 공약인 곧 발표될 국가 복원력 전략은 국가 복원력에 대한 가장 중요한 접근법을 제시할 것이다.

89. 국가 사이버 보안 센터(NCSC)의 설립과 함께, 자문, 지침 및 기타 수단의 가용성 증가, 네트워크 & 정보 시스템 규정(NIS 규정), 일반 데이터 보호 규정, 2018년 데이터 보호법을 포함한 법률의 시행 등 지난 10년 동안 사이버 복원력 개선에 상당한 진전이 있었다. 그러나 여전히 심각한 개선 숙제가 남아 있다. 사이버 침해는 정부, 기업, 조직 및 개인에게 영향을 미치고, 많은 기관에서는 여전히 다수의 사이버 보안 침해 또는 공격이 보고되고 있다.

90. 우리는 이전 전략서의 토대 위에서, 접근 방식을 발전시키며, 다음 사항에 중점을 두고 영국의 사이버 복원력에 대한 방향을 전환한다.

- 우리의 활동을 확대하여 인터넷을 자동적으로 안전하게 만들고, 공격을 방지하며 모든 영국 기업, 조직 및 시민들에게 이익을 주기 위한 기본 보호 장치를 구축하고, 온라인에서 자신을 보호할 수 없는 사람들을 지원

- 정부가 사이버 보안에서 최고의 모범적 사례가 되기를 목표로 삼는다.

- 규제 및 기타 장려책의 더 효과적으로 사용하여 사이버 보안을 이상적 사업의 핵심 부분으로 자리매김하게 하고, 우리의 위협 통찰력을 활용하여 스스로를 방어할 수 있는 커뮤니티를 구축

- 객관적으로 측정 가능한 기준, 증거 및 데이터로 이 모든 것을 뒷받침하고 데이터를 수집하기만 하지 않고 데이터를 이용하여 그에 따라 조치하는 방향으로 전환.

91. 이 전략에서 사이버 복원력의 개념은 세 가지 주요 측면이 있다. 첫째, 위험의 본질을 이해해야 한다. 둘째, 사이버 공격을 예방하고 저항할 수 있는 시스템을 구축하기 위한 조치가 필요하다. 셋째, 일부 공격이 여전히 발생할 수 있다는 점을 인지하고, 이러한 공격에 대비해야 하며, 피해를 최소화하고 복구할 수 있도록 충분히 복원력있게 대응해야 한다.

92. 우리의 접근 방식은 우리가 시스템 위험을 해결할 수 있도록 지원하는 국가 역량으로 받아 각각의 대상에 맞게 조정될 것이다. 우리가 보호하고 영향을 미치려고 하는 대상들은 영국 시민들, 기업들, 기관들, 정부 및 공공 부문, 그리고 우리의 중요한 국가 기반 시설을 운영하는 사람들이다. (우리 모두에게 꼭 필요한 식수, 전기, 금융, 교통, 통신과 같은 핵심 서비스 제공하는 기반시설).

93. 우리는 우선 첫째로 모든 영국 인터넷 사용자의 디지털 환경 확보, 공격 방지, 제품 및 서비스의 기본 보안 구축, 그리고 개인 및 소기업과 기관의 사이버 보안 개선을 위한 기본 조치 지원에 초점을 맞출 것이다. 그리고 더 큰 책임과 능력을 가진 기관들 대상으로는 위협에 비례하는 보안과 복원력의 추가적 조치가 가능하게 할 것이다. 이는 결국 우리 국민과 경제가 의존하는 주요 공공 및 필수 서비스에 필요로 하는 최고 수준의 보호로 귀결될 것이다.

94. 이것은 정부와 경제, 사회의 모든 부분과 공동의 노력이어야 한다. 기업 및 기관의 이사회는 사이버 위험을 자체적으로 관리할 책임이 있다. 우리의 목표는 개선을 가능하게 하는 장려책, 지원 및 규제의 올바른 틀이 뒷받침하는 명확한 기대치를 설정하고 사이버 보안 위험의 부담을 최종 사용자로부터 이를 대처하기 가장 적합한 위치에 있는 사람들에게 이양하는 것이다.

95. 우리는 정부 부처, 모든 공공 부문 및 중요한 국가 인프라(CNI)의 규제 운영자들이 기준을 높이고 위험을 보다 능동적으로 관리할 것을 요구한다. 우리는 디지털 서비스 및 플랫폼 공급자를 포함한 대기업과 기관이 사업 운영의 핵심 부분으로서 시스템, 서비스 및 고객을 보호하는 데 더 많은 책임을 지기를 기대한다. 그 대신 정부는 디지털 환경 확보와 시스템 위협 해결, 자문, 수단, 시장 인증, 개선이 가능한 기술 개발 등을 통해 지원을 아끼지 않을 예정이다.

96. 영국이 사이버 복원력을 촉진하기 위한 노력으로 반드시 우리의 국제적 협력을 또한 이끌어 내야 한다. 공급망, IT 플랫폼, 다국적 기업, 인터넷 자체의 세계화가 심화되고 있다는 것은 우리가 혼자서는 영국의 사이버 보안을 개선할 수 없다는 것을 의미한다. 이 과제를 해결 하기 위해서는 영국과 국제 사이버 복원력 사이의 연관성에 대한 인식을 높이고, 위험성이 높은 영역을 해결하며, 전략 축 4: 글로벌 리더십 장에서 제시하는 상호 이익을 위한 디지털 변환, 보안 및 무역을 가능하게 하는 복원력을 구축 하기 위해 국제 파트너와 협력해야 한다.


모든 사람의 부담을 덜어준다.
영국 인터넷 사용자를 보호하고 시민들을 위한 온라인 서비스의 기본적 보호망을 제공하기 위해 업계와 협력한다.
적극적 사이버 국방을 확대하고 사이버 범죄와 사기를 방지하고 해체한다.
기업과 기관의 복원력을 높힌다.
사이버 필수와 같은 기준과 투명성, 시장 인센티브와 지역 지원을 높힌다.
디지털 서비스와 개인 정보를 포함한 목표 분야의 더 좋은 규제를 마련한다.
공공 서비스의 복원력을 높힌다.
2030년까지 이미 알고 있는 공격 방법에 대응하는 복원력을 갖춘다.
책임 소재, 기준과 독자적 확약을 증대한다.
전통 IT에의 투자를 증대한다.
필수 국가 기반 시설의 복원력을 높힌다.
일반적 공격 방법에 대해 복원력을 갖추고 리스크 종류에 따른 선진적 보호를 준비한다.
디지털화와 신기술로 인하여 발생하는 리스크를 알리고 이해한다.

목표 1:
사이버 위험에 대한 이해를 개선하여 사이버 보안 및 복원력에 대한 보다 효과적인 조치를 추진한다.

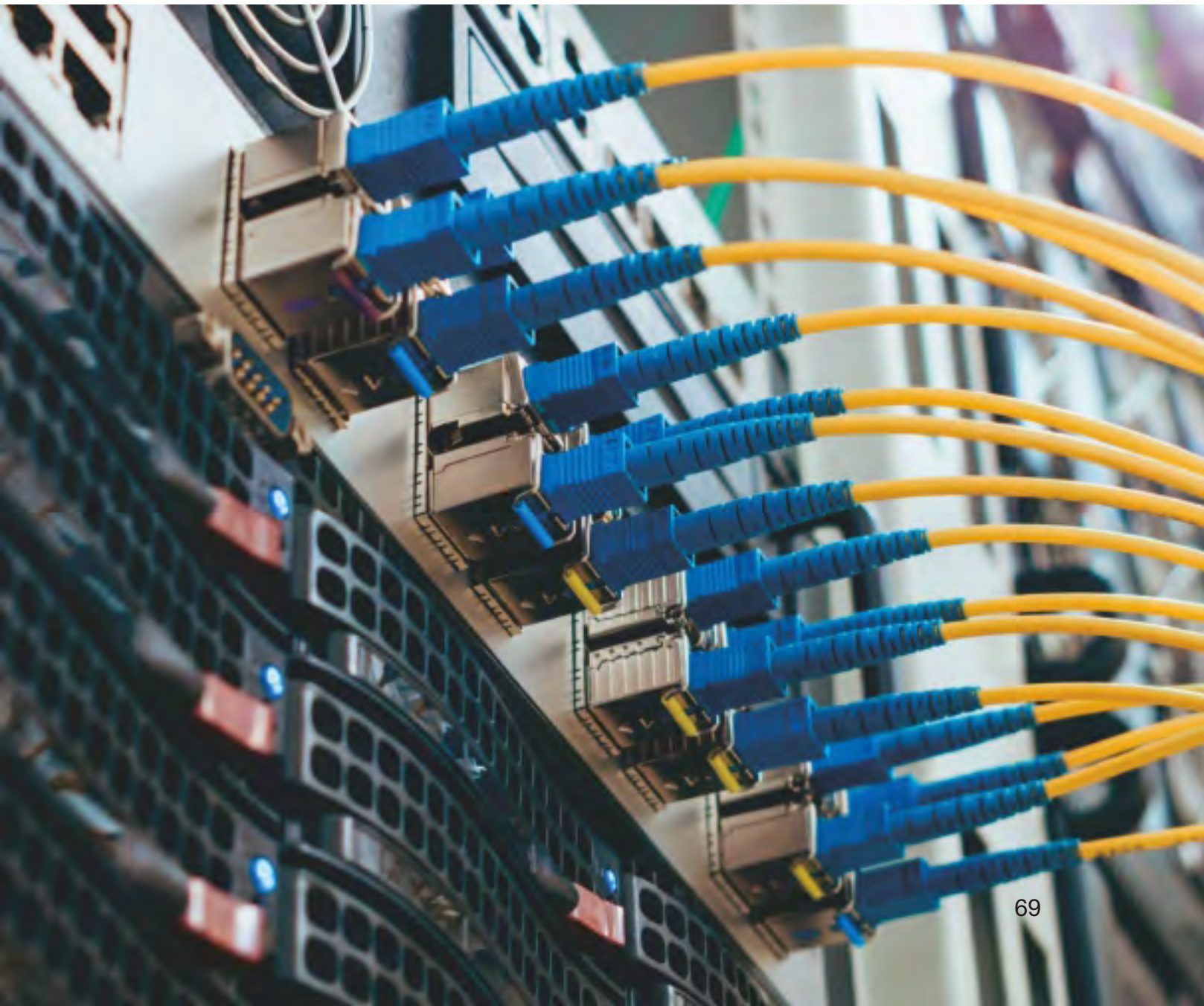
97. 우리는 위협에 대한 공동의 이해를 높이고, 우선 순위 결정을 인도하며, 조치 사례를 확립하기 위해 정부, 기업 및 기관 간에 훨씬 더 긴밀한 협력을 할 것이다. 우리는 소비자에게 서비스를 제공하는 기업 및 기관과 협력하여 국민을 지원할 것이며; 최고로 중요한 위험을 식별하는 정부의 능력을 더욱 강화할 것이다. **우리는 2025년까지 다음과 같은 성과를 달성할 것이다:**

98. 정부는 국가의 사이버 위험에 대한 최신의 전략적 이해를 하고 있으며, 이 이해를 이용하여 시스템적 위험을 식별하고 우선 순위를 소통하고 전략과 전달을 주도한다. 우리는 이전 국가 사이버 보안 전략의 '위협을 이해'하기 위한 상당한 투자로부터 더 많은 가치를 유지하고 이끌어 낼 것이며, 점점 더 상호 연결되는 세상에서 위험을 이해하기 위한 기존 노력 위에서 만들어 갈 것이다. 여기에는 디지털 공급망이 지나치게 집중된 곳을 파악하고, 국제 협력사와 협력해 공통 위협에 대처하는 내용이 포함될 예정이다. 우리는 또한 컴퓨터 오남용법(CMA) 위반에 대한 기록을 개선하고, 데이터 침해와 후속 범죄 사이의 연관성을 이해하며, CMA 위반이 다른 유형의 범죄 활동을 어떻게 유발하는지에 대한 분석을 할 것이다.

99. 정부는 사이버 위험에 대한 이해에서 모범전 선례가 되고 있다. NCSC의 사이버 평가 체제(CAF)를 모든 정부 부처의 보증된 체제로 채택하고, 중요 시스템과 공통 공급 업체에도 공유할 예정이다. 우리는 새로운 정부 사이버 조정 센터(GCC)와 정부 간 취약성 보고 서비스(VRS)를 설립하여 정부가 사고, 취약성 및 위협을 대처할 때 '통합된 방어'를 할 수 있도록 할 것이다. VRS는 정부 기관 전체의 취약점 감소를 통해 보안 연구원 단체와의 가치 있고 신뢰할 수 있는 관계를 목표로 할 것이다. 우리는 또한 스코틀랜드의 사이버 복원력을 위한 중앙 조정 기능 설립 제안과 같이 위임된 정부에서도 유사한 계획을 지속적으로 지원하고 조정할 것이다.

100. 영국 CNI 전반에 걸쳐, 우리는 사이버 위험에 대해 더 정교한 이해를 하고 CNI 부문에 걸쳐 사이버 평가 체제(CAF) 또는 동등한 체제의 채택을 늘리고 사용 중인 다른 사이버 보안 체제 및 보고 체계와의 연계성을 개선할 것이다. 우리는 위험성 검토를 완료하고 CNI와 공급망 내의 의존성을 측정할 것이다. CNI 소유자 및 운영자와 더욱 강력한 협력을 구축하여 위협 및 리스크 정보에 대한 접근성을 개선하고 리스크 대응 태세를 동의할 것이다. 또한 Net Zero로의 전환과 같은 보다 광범위한 우선 순위의 일부분을 포함하여 새로운 CNI가 디지털화와 신기술의 결과로 부상하고 있는 분야 또는 새로운 리스크를 이해하기 위해 노력할 것이다.

101. 영국 기업과 기관은 사이버 위험과 이를 관리할 책임을 잘 이해하고 있다. 우리는 기관이 보유한 데이터가 사기, 신원 도용 또는 탈취와 같은 범죄를 촉진하는 데 어떻게 사용될 수 있는지를 포함하여 기관이 고객에게 미칠 수 있는 위험을 더 잘 인지할 수 있도록 지원한다. 그리고 우리는 사이버 공격의 확산과 영향에 관한 연구와 정보을 통해 얻은 통찰력을 널리 공유하고 관련 진행 부문이 사이버 보안을 개선하는 과정에서 얻은 통찰력을 공유할 것이다.



목표 2:
영국 기관 내의 사이버 위험 대처를 개선하고 시민을 보다 효과적으로 보호함으로써 사이버 공격을 방지하고 저지한다.

102. 사이버 공격을 방지하고 저지하기 위한 우리의 접근법은 다음과 같다: (i) 기관은 자체적인 사이버 위험을 대처하기 위한 조치를 취해야 할 책임이 있지만, 이것을 우선 순위로 만들기 위해 이사회 차원에서 더 강력한 의무 체제와 좋은 관리 방식이 필요하다; (ii) 정부가 업계와 협력하여 위협을 줄이기 위해 직접적으로 가담해야 할 역할이 있다; (iii) 개인, 개인 및 소규모 사업자와 기관이 그들의 사이버 위험에 대처할 수 있도록 지원 및 지침이 제공되도록 보장해야 한다. **우리는 2025년까지 다음과 같은 성과를 달성할 것이다:**

103. 정부는 영국에 미치는 피해 규모를 줄였고 영국 국민들의 부담을 줄여 왔다. 우리는 자선단체, 학계 및 중소 기업 및 국민을 포함한 광범위한 분야를 지원하기 위해 "적극적 사이버 방어" 조치를 확대하면서 영국의 모든 인터넷 사용자를 위해 조치를 더 확산할 것이다. 그리고 업계와 업무 확대와 정보 공유를 통해 온라인 서비스에 대한 보호를 강화할 것이다.

104. 이러한 활동은 사기와 같은 경제 범죄에 대응하기 위한 정책과 온라인 안전법 초안과 같이 영국의 국민을 온라인에서 보호하기 위한 정부의 우선 순위를 보완하기 위한 정책이다.

105. 즉, 온라인 서비스 제공자, 통신, 기술, 은행 및 소매업 등 관련 분야와 더 긴밀하게 협력하여 불법적인 목적으로 웹사이트를 등록하는 것을 더 어렵게 만들고, 온라인 악성 콘텐츠의 제거와 차단을 증가시키며, 도난 당한 신용증명을 복구 및 반환, 그리고 영국의 통신 시설 보안을 강화하는 것을 포함한 영국 인터넷 사용자 보호를 증진 시키는 것이다. 우리는 자발적 대응이 불충분한 경우 국민의 보호를 위해 법적 지원이 가능하도록 방법을 개발할 것이다.

106. 피해를 줄이기 위한 우리의 노력에는 디지털 공급망의 시스템적 위험을 해결 하는 것을 포함한다. 우리는 중요 부문에서 외국인 직접 투자 심사에 관한 정보 공보 공유 개선과 강력하고 예측 가능한 비례적인 접근법을 통해 공동 경제 보안을 강화 하고, 정부 기관의 주요 공급자에게 명확한 요구사항을 설립할 것이다.

107. 정부의 중요한 기능들은 사이버 공격에 대응력을 크게 강화하고 2030년까지 공공 부문의 모든 정부 기관이 이미 알려진 취약점과 공격 방법에 능동적으로 대처할 것이다. 우리의 목표는 영국의 공공 부문을 모범 사례로 확립하는 것이다. 이 결과로 인해 우리는 최초의 정부 사이버 보안 전략을 발표 할 것이다. 이 전략은 보다 효과적인 위험 대처 과정, 관리 및 책임; 중심적으로 개발 및 채택된 기능(능동 사이버 방어 포함); 시스템, 네트워크 및 서비스에 대한 보다 종합적인 모니터링; 신속하고 확장된 사고 대응; 지속 가능성을 촉진하는 기술, 지식 및 문화에 대한 투자에 초점을 맞출 것이다.

108. 영국의 중요한 국가 기반 시설에 대한 사이버 위험은 더욱 효과적으로 관리될 것이다. 이 기반 서비스들은 정의적으로 국가가 가장 많이 의존하는 서비스들이다. 우리는 운영자와 지속적으로 긴밀히 협력하여 일반적인 공격 방법에 대한 복원력을 최대한 신속하게 달성하고 필요한 곳에 더 고급의 보호 기능을 배치할 것이다. NIS 규정에 따라 지정된 필수 서비스 운영자의 경우, 최소한 각 부문에 대해 관련 관할 기관이 설정한 기초 표준을 충족해야 한다.

109. 이를 위해 정부는 CNI 운영자가 중요 시스템의 사이버 보안에 투자하고 그들의 공급망을 포함한 모든 곳에서 일어날 수 있는 위험을 효과적으로 대처할 수 있는 능력을 검토할 것이다. 우리는 광범위한 국가 안보 위험과 급변하는 위협과 기술의 맥락에서 적용 범위, 권한 및 적응력을 향상시키기 위해 규제 체제를 강화할 것이다. 이는 NIS규제 개혁에 대한 협의, 영국 통신사들을 위한 새로운 보안 체제 시행, 그리고 영국이 넷 제로를 실행하기 위해 필요로 하는 미래의 스마트하고 유연한 에너지 시스템이 사이버 위협에 안전하고 복원력 있을 수 있도록 하기 위한 비례적 규제 체제 개발로 시작될 것이다.

110. 이와 함께 우리는 규제 기관의 역량 강화; 사이버 전문가(참조: 영국 사이버 생태계 장)를 유치, 개발 및 유지하는 CNI 사업자의 능력 향상을 위한 역량에 투자; 중요 공급 업체와의 참여를 강화하여 운영자들의 공급망 위험 대처를 지원하고 지침에서부터 입법 및 조달 관련 제안에 이르는 모든 범위의 수단을 분석할 것이다.

111. 우리의 데이터 사용을 의존하는 기반 시설은 안전하고 복원력 있다. 이러한 시설은 국가적 필수 자산으로, 경제를 지원하고 공공 서비스를 제공하며 성장을 촉진한다. 우리는 정보가 외부 데이터 센터를 포함한 모든 곳에서 처리, 전송 또는 저장될 때 충분히 보호되도록 하는 데 더 큰 역할을 할 것이다. 부문 전반에 걸쳐 보다 높은 보안성과 복원력 기준을 확보할 수 있도록 보다 강력한 위험 대처 틀을 구축하고, 2021년 국가 보안 투자법 조항을 시행해 투자 심사를 강화해 나갈 것이다. 글로벌 정보 접근 및 유동성 증가가 영국이 직면한 보안 위험을 증가시키지 않도록 국제 파트너와의 협력을 강화하고 대량 데이터 수집으로 인한 보안 과제도 해결할 것이다.

112. 우리는 또한 중요한 국가 기반 시설 내에서 경제와 그 역할을 뒷받침하는 영국 데이터 기반 시설 서비스의 증가하는 중요성에 대해서도 숙고를 할 것이다. 이러한 조치는 국가 데이터 전략 및 통합 검토에 명시한 책무와 맥을 같이 한다.

113. 더 많은 영국 기업과 기관이 사이버 위험에 사전 대비하여 대처하고 사이버 복원력을 개선하기 위한 조치를 취하고 있다. 우리는 효과적인 사이버 보안을 장려하는 시장 장려책 개발을 통해 지원 및 행동 변화를 추진하겠다. 필요한 경우, 이것은 관련 법률을 보완하여 사이버 위험을 가장 큰 책임이 있는 사람들이 효과적으로 대처하는 것을 보장할 것이며, 영국의 사이버 보안 법률이 진화하는 위험과 기술에 효과적으로 대응할 수 있도록 할 것이다.

114. 이러한 목표를 지원하기 위해, 우리는 경제 전반에 걸쳐 우수한 사이버 보안 관행을 장려하기 위해 시장 영향력 행사자(생산자, 금융 기관, 투자자, 회계 감사 및 보험사)와 점점 더 협력할 것이다. 우리는 사이버 위험 등 위험에 대한 복원력 공동 보고에 대한 개선 사항을 제안할 것이다. 이를 통해 투자자와 주주들은 기업이 사업에 미치는 중요한 위험을 어떻게 대처하고 완화하고 있는지에 대한 통찰력을 높일 수 있을 것이다. 그리고 사이버 핵심 사항 증명 제도와 같은 인증 및 기준 획득을 지속적으로 촉진하고, 사이버 위험 대처에 이사회 차원의 참여를 촉진할 것이다.

115. 관련 법률은 주로 특정 필수 제품 및 디지털 서비스 제공업체, 광범위한 경제에서의 데이터 보호 및 대기업을 포함하여 사이버 공격의 잠재적 영향이 가장 큰 부문에 초점을 맞출 것이다. 이는 위에, 기술 챕터, 그리고 개인 데이터 보호를 위한 영국의 체제를 개혁하기 위한 다음 단계에 설명된 바와 같이 네트워크 및 정보 시스템(NIS)의 보안을 관리하는 규정에 초점을 맞춘 디지털 규제 계획을 보완할 것이다.

116. 영국 기업 및 기관 전반에 걸친 비즈니스 복원력과 사이버 보안을 개선하기 위해 취할 조치에 대한 자세한 내용은 사이버 보안 규정 및 장려책 검토 부분에서 제시할 예정이다.

117. 사이버 복원력 향상을 위한 기술 자문, 자구적 도구 및 보장된 제품과 서비스는 접근 쉽고 지속적으로 개선되며, 특히 시민, 개인 사업자 및 소규모 기관 지원에 중점을 두고 있다. 우리는 NCSC를 통해 기술적으로 정확하고 시기 적절하며 실행 가능한 지침과 자구적 도구를 계속 개발할 것이다. 우리는 사이버 인식 캠페인, NCSC 웹 사이트, 정부, 법 집행 네트워크 또는 업계 파트너십과 같은 가장 효과적인 채널을 통해 전달하고자 하는 바를 일관되고 명확하며 제공할 수 있도록 할 것이다; 그리고 우리는 지역 단위에서 가능한 지원을 더 할 것이다. 우리는 학습자들이 온라인에서 안전하고 책임감 가지고 사용하도록 하기 위한 기본적인 디지털 능력을 보장하기 위해 '디지털 자격 부여'를 통해 필요한 성인들을 위한 필수 디지털 능력 자격에 전액 지원할 것이다. 또한 기업과 기관이 복잡한 사이버 보안 시장을 탐색하고, 보장된 제품과 서비스에 대한 우리의 틀을 확장하며, 소기업들이 기본적인 조언을 쉽게 접할 수 있도록 사이버 관련 필수 사항을 중심으로 상업적으로 제공할 수 있는 사항을 개발할 수 있도록 지원할 것이다.

Elis Power
타리안 지역 사이버 범죄 수사대
사이버 보호/방지 경찰관

타리안 지역 사이버 범죄 수사대는 웨일스 경찰에서 파견된 여러 분야의 걸친 경찰 조직이다. 그들의 임무는 남웨일스의 더 안전한 사이버 환경 제공에 기여하는 것이다.

사이버 보호/방지 담당 경찰관 Elis Power는 참여 팀에서 근무하고 있다.

"뻔한 말이지만, 수사대에는 평범한 날은 하루도 없다. 나는 매일 내부 경찰 부서 또는 외부 기관이 사이버 위협으로부터 자신과 업무 공간을 보호하는 방법을 확실히 이해하도록 조언이 담긴 프레젠테이션을 해야할 책임을 지고 있다. 나는 또한 학교의 청년들에게 인터넷 안전에서부터 1990년 컴퓨터 오용법에 이르기까지 다양한 주제에 대해 발표하기도 한다. 나는 협력 기관 및 군대와의 회의에 자주 참석하여 새로운 위협 요소 및 관련 지침을 논의한다. 또한 취약점 경고를 받는 기관들과 접촉하고, 국가 운영에 참여하고, 관련 이벤트 및 회의에 게스트로 참석하고, 지속적으로 내 능력과 지식 기반을 개발할 수 있는 시간을 갖기도 한다."

목표 3:
사이버 공격에 대비, 대응 및 복구하기 위한 국가 및 기관 차원의 복원력 강화

118. 리스크를 이해하고 예방 조치를 취하려는 노력에도 불구하고 몇몇 사고는 여전히 발생할 것이다. 우리는 모든 기관에 걸쳐 사고 관리 및 대응 능력을 강화하고, 그로 인한 피해를 최소화하고, 피해자에게 더 나은 지원을 제공해야 한다. **우리는 2025년까지 다음과 같은 성과를 달성할 것이다.**

119. 국가적으로 중요한 사이버 사고 대응에 대한 영국의 전략적 대처와 조정은 전보다 훨씬 더 효과적이다. 우리는 중요한 사이버 사고에 대응한 정부의 경험을 바탕으로 얻은 교훈이 정책과 과정을 개선하는 데 활용되도록 할 것이다. 우리는 국제적 협력 관계의 파트너들 및 업계와 위기 관리 경험을 공유하고, 다른 곳에서의 모범 사례를 발굴하여 우리의 대비와 과정을 강화해 나갈 것이다. 우리는 NCSC 및 법 집행 사고 관리 팀이 진화하는 모든 유형의 사건 사고에 대응하고 우선 순위 위협에 대한 국가 차원의 대응을 조정하는 데 필요한 전문 지식과 수단을 갖추도록 준비할 것이다.

120. 사이버 사건을 보고하는 것이 더 쉬워지고 사이버 범죄의 피해자들은 더 나은 지원을 받는다. 또한 보고된 정보는 미래의 사건들을 예방하고 사이버 범죄자들을 수사, 방해, 기소하기 위한 법 집행을 지원하는 데 사용될 것이다. 이를 지원하기 위해 2025년까지 새로운 국가 사기 및 사이버 범죄 보고 및 분석 서비스를 제공할 것이다. 우리는 런던 경찰의 새로운 업무 보고 능력을 포함하여 여러 방법으로 사이버 사고에 대한 보고를 더 많이 장려할 것이다. 규제 부문에서는 규제 기관이 '거의 일어날 뻔한 사고'를 포함한 광범위한 사고에 대한 보고를 요구할 수 있도록 할 것이다. 이번 국제 경제 범죄 피해자 복구 부서 출범으로 어렵고 유해한 경험을 겪은 피해자를 위한 지원과 지침을 개선할 것이다.

121. 정부와 CNI는 더 나은 사고 계획 및 정기적인 훈련을 통해 사고에 대응하고 사건으로부터 복구하기 위해 더 많은 준비를 하고 있다. 우리는 사이버 사고 대응을 위한 NCSC의 인증 제도를 확대하고, 새로운 훈련 체계를 소개함으로써 정부와 CNI 운영자가 시장에서 필요한 사이버 훈련과 사고 관리 서비스에 접근이 용이하도록 도울 것이다.

122. 정부 내에서는 부서 내 및 정부 디지털 부동산 전반에 걸쳐 모니터링 및 탐지 기능이 향상될 것입니다. 우리는 정책 및 프로세스를 개선하고, 국제적 파트너 및 업계와 위기 관리 경험을 공유하며, 사고 관리 팀이 진화하는 모든 유형의 사고에 대응할 수 있는 필요한 전문 지식, 역량 및 능력을 갖추도록 보장할 것입니다.

123. CNI 내에서 우리는 CNI 운영자에 걸친 훈련 및 테스트 또는 적 시뮬레이션을 위한 명확한 조건을 정하고, 금융 부문 사이버 협업 센터와 같은 모델의 적용을 고려하여 사고 대응 및 훈련의 혁신과 협업을 촉진할 것이다. 또한 기술에 대한 우리의 목표의 한 부분으로 (다음 장에 요약됨) 업계, 학계 및 국제 협력 파트너들과 협력하여 이 분야에서 능력을 구축하기 위한 중요한 산업 기술에 대한 테스트, 훈련 및 교육을 위한 우수 센터로서 운영 기술 보안을 위한 국립 연구소를 설립할 것이다.

124. 영국 기업과 기관은 사고가 발생했을 때 무엇을 해야 하는지, 누구에게 연락해야 하는지, 누가 도와줄 수 있는지, 어떻게 복구해야 하는지에 대해 보다 명확하게 이해하고 있다. 우리는 새로운 사이버 사고 대응 체계와 사이버 사고 훈련 서비스를 포함한 보증된 업계 서비스의 지원을 받아 훈련에 대한 접근성을 개선할 것이다. 우리는 사이버 범죄의 개별 피해자에 대한 일관된 전국적인 법률 집행 지원에 대한 접근을 보장하고, 중소기업과 기관이 지역 사이버 복원 센터와 같은 지역 지원을 활용할 수 있도록 장려할 것이다.

Daniel Ng, CEO, CyberOwl
CyberOwl 대표

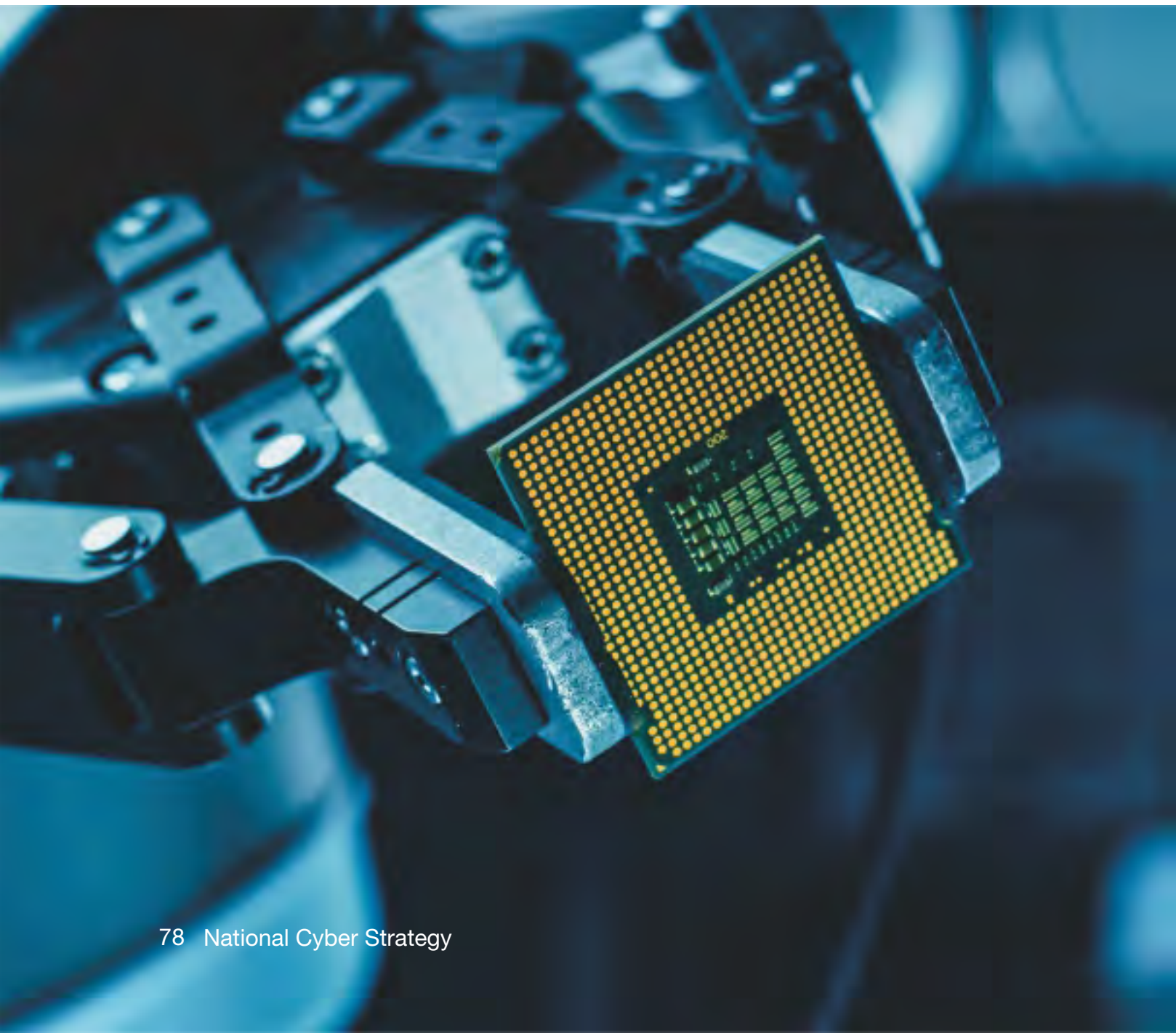
CyberOwl은 정부의 사이버 개발 프로그램의 혜택을 받았다. 우리는 해양 및 CNI 분야의 운용 자산에 대한 사이버 보안 모니터링 및 분석을 제공한다. 지속 가능성을 확보하기 위해서는 현장 자산의 연결성과 디지털화가 더욱 요구되어 결국 사이버 위험에 노출된다. CyberOwl은 운영자가 자산을 식별 및 매핑하고, 사이버 위험에 대한 조기 경고를 받고, 그들 자신과 규제 기관에 이를 확보 했음을 입증할 수 있도록 한다. 우리는 글로벌 해운 물류 공급망의 복원력을 향상시키기 위해 EMEA(유럽 중동 아프리카) 및 아시아 태평양 지역의 세계 최대 해양 자산 운용사들과 협력하고 있다. 2021년에 우리는 영국과 싱가포르에서 예약 건수를 14배 늘리고 영업 건수를 두 배로 늘렸다.

Jen Ellis, Vice President of Community and Public Affairs, Rapid7
Rapid7사 공보 담당 부사장

나의 업무는 모든 규모와 분야의 보안 전문가 및 리더와 대화하여 당면한 과제를 이해하고 사이버 보안을 강화할 수 있는 해결책을 찾는 것이다. 나는 조직이 과부하 되어 어디에 집중해야 할지, 어떻게 시작해야 할지, 어떻게 진행해야 할지 모르겠다는 이야기를 꾸준히 듣고 있다. 기술 직원이 대표의 승인을 받는 것도 어려울 수 있다. 정부가 명확하고 일관적이며 투명한 사이버 전략을 가지고 있으면 이를 해결하는 데 도움이 될 수 있다. 이러한 정부의 사이버 전략을 가지고 기술 담당자가 사장단과의 대화에서 효과적으로 토론을 할 수 있을 것이고 또한 집중해야하는 중점 영역과 완성으로 가기 위한 잠재적 경로를 파악하는데 도움이 된다. 사이버 보안은 아직 굉장히 복잡하고 끝이 없지만, 광범위한 사이버 전략을 통해 사이버 보안의 중요성에 대한 이해와 우리 모두 함께 한다는 생각을 가질 수 있을 것이다.

전략 축 3:

기술적 이점



사이버 전력에 필수적인 기술 선도

125. 일부 기술은 사이버 공간의 미래를 형성하는데 핵심적인 역할을 할 것이다. 이러한 기술에서 선도적 역할을 확립할 수 있는 국가는 디자인과 활용방식에서 유리한 위치를 선점하고 자국의 보안 및 경제적 이점을 효율적으로 보호할 수 있으며, 사이버 능력의 획기적인 발전 기회를 더 빨리 활용할 수 있다. 기술이 지정학적 세력을 형성하는 데 점점 더 중요한 수단이 되면서 이 분야의 경쟁은 더욱 치열해질 것이다.

126. 과학 기술을 통한 전략적 우위와 관련 데이터에 대한 접근성 확보가 영국의 사이버 강국으로서 포괄적 목표달성을 위한 전제 조건이 될 것이다. 지금까지 영국 정부는 스타트업 양성 프로그램 과 사이버 안보연구 센터(Academic Centres of Excellence in Cyber Security Research)등을 통해 사이버 안보 기술 혁신을 지원하고 "애초에 안전하게 설계된" 소비자용 온라인 기기들의 개발을 장려하는 전략을 취해왔다. 그러나 이제 영국은 경쟁국과 적국에 지나치게 의존하게 되는 상황을 피하고 핵심 기술 지분 확보를 위해 더 적극적이고 야심찬 정책 접근 방식이 필요하다..

127. 통합 검토서(Integrated Review)는 영국을 과학 기술 초강대국으로 만들고 우리의 전략적 우위 구축과 유지를 위해 과학 기술을 적극 활용하는 계획을 세웠다. 이는 인공지능, 양자 기술 및 데이터와 같은 분야에서 영국의 전략을 완성하고 '국가 과학기술 위원회'와 '과학 기술 전략 사무국'을 지원한다.

128. 국가사이버안보센터(NCSC)와 정부 부처의 기술 전문지식을 중심으로 사이버 전력에 가장 핵심적인 기술 분야를 파악하는 역량을 강화한다. Integrated Review에 명시된 '자체 협력 접근' 시스템내에서 작업하면서 우선 순위에 대한 국가 차원의 전략적 결정을 내릴 것이다. 선별된 분야에서 영국 국내 역량 개발을 위해 필요한 R&D와 전략적 파트너십에 투자할 것이며, 국제 시장에서 신뢰할 수 있는 다양한 공급망 형성을 장려하고 과학 기술이 개방되고 안전하게 활용될 수 있는 표준을 확립하기 위해 산업계, 규제 기관과 국제 파트너들과 협력할 것이다. 또한 영국 경제 사회 이익의 극대화를 위해 국가 데이터 전략에 명시된 프레임워크를 기반으로 신흥 기술 혁신을 추진하고 이와 함께 발생 증가하는 데이터와 정보를 활용하고 보호하는 영국의 역량을 강화할 것이다.

사이버 강국을 위한 핵심 기술

다양한 신기술 및 기존 기술이 영국의 사이버 강국 부상에 필수적일 것이다. 또한 우리는 이러한 기술 개발을 예상하고 평가하고 발전시킬 수 있어야 한다. 아래 명시된 바와 같이 우리의 전략을 실행하기 위해 다양한 기술과 활용에 대한 우선 순위를 정할 것이다. 이는 완전히 확정되어 불변적인 것이 아니라 산업계, 학계와 기술전문가들과 협의하여 지속적으로 발전해 나갈 것이다.

- G 및 6G 기술 및 기타 새로운 형태의 데이터 전송
- 인공지능(AI) , AI시스템 확보와 네트워크 모니터링과 같이 광범위하게 AI를 활용하여 사이버 안보를 강화하는 방안 확보
- 블록체인 기술과 암호 화폐 및 탈중앙화 금융과 같은 블록체인 기술 활용
- 반도체, 마이크로프로세서 칩, 마이크로프로세서 아키텍처 및 공급망, 설계 및 제조 프로세스
- ID 및 액세스 관리와 높은 보안 암호화 제품을 포함한 암호화 인증
- 연결된 장소와 같이 소비자, 기업, 산업 및 물리적 환경에서 사용되는 사물 인터넷(IoT) 및 관련 기술
- 양자 컴퓨팅, 양자 감지 및 사후 양자 암호학을 포함한 양자 기술

이 작업은 국가 데이터 전략, 국가 AI 전략 및 The Integrate Review를 포함한 영국 정부 부처 전반의 다양한 전략과 과학기술 중심 목표의 설정과 이행과 일치하며 이를 지원한다.

목표 1:
사이버 강국에 핵심적인 과학 기술 개발을 예측, 평가 발전시킬 역량 강화

129. 사이버 관련 기술 경쟁력을 확보하고 유지하기 위해서는 과학기술의 핵심 분야를 식별 및 분석 하여 국가 우선순위로 선정하고 노력하는 일관되고 통합적이며 확고한 접근 방식이 필요하다. 이를 위해서는 정부, 학계를 포함한 폭넓은 기관들과의 연구와 기술 전문 지식을 더욱 발전시켜야 할 것이다. 이와 함께 국제 파트너들과 경쟁국들의 우선 순위와 시스템을 파악하기 위해 해당 산업전문가들의 분석에 집중 하고 해외 네트워크를 활용하여 과학, 기술, 정보를 아우르는 새로운 정부 조직을 출범할 것이다. **영국은2025년까지 다음과 같은 성과를 이룰 것이다:**

130. 정부는 새롭게 발전하는 과학기술을 분석하여 이들이 영국의 사이버 정책과 전략에 미치는 영향을 잘 파악하고 있다. 영국은 과학청(Government Office for Science)과 그 외 기관들의 전문가들과 협력하여 연계 장소 (connected place), 교통과 같은 분야의 신흥 기술에 집중하고 NCSC의 맨체스터 신규 활용 연구 거점과 같은 연구 역량을 확대해 나갈 것이다. 영국은 정부이 외의 기관에서 전문성을 확보하기 위해 사이버 안보연구소 4곳과 사이버 안보연구센터 (Academic Centres of Excellence in Cyber Security Research) 19곳, 우선 순위 주제 연구자를 위한 Pathfinder상을 지원하고 해외 활동과 국제 파트너십을 보다 효과적으로 활용할 것이다.

131. 이렇게 개선된 상황 인식으로 정부의 새로운 분야 정책 결정과 우선 순위 선정을 보다 빠르고 효율적으로 할 수 있고 기회 포착과 위험 요소 완화를 위해 보다 사전 예방적인 접근법을 취할 수 있게 되었다. 새로운 미래 예측 연구를 통해 과학 기술의 발전과 이들이 사이버에 미치는 영향을 연구 하는 조직을 구축할 것이다. 이를 바탕으로 영국 안보 이익을 위한 핵심 사이버 기술, R&D 및 정책 개발 우선 순위가 결정되고 과학기술 전략실(Office for Science and Technology Strategy)과 국가과학기술위원회 (National Science and Technology Council)에도 광범위한 정책 결정을 위해 공유될 것이다.

Máire O'Neill
정보보안기술 연구소 (CSIT), 수석 조사관

CSIT는 대학에 속해 있는 사이버 안보 기술 연구 센터중 영국에서 가장 규모가 큰 곳 중 하나이다. 마이어 오닐 교수가 소장인 이 연구소는 2009년 영국 최초 혁신 지식 센터 중 하나로 선정되었다. 지난 10년동안 CSIT는 성공적인 연구, 혁신, 산업계와 협업으로 국내외적으로 명성을 쌓으며 괄목할 만한 성장을 해왔다. CSIT는 스핀아웃(전문회사 설립), 지역 자생기업 지원, 외국인 직접투자 유치와 같은 활동으로 북아일랜드 사이버 안보 클러스터 성공의 결정적인 역할을 해왔다. 2009년에 시작된 북아일랜드의 사이버 산업은 현재 104개 기업, 2,300명 고용, 매년 1억 1천만 파운드의 급여를 창출하고 있다.

목표 2: 사이버 공간 핵심 안보 기술의 주권적 동맹적 우위 확보 및 유지

132. 사이버 기술 핵심 분야에서 선도적인 위치를 선점하거나 경쟁 우위를 확보할 수 있는 잠재력이 있는 분야 또는, 비동맹 공급원에 대한 의존으로 용납할 수 없는 안보 위험을 초래하는 경우, 영국은 국내 산업 기반을 발전시키는 방안을 모색할 것이다. 진정한 주권 역량을 유지해야 하는 부분도 있고, 국제 파트너들과 협력하거나 국제 시장의 일정 분야에서 선도적인 위치를 모색해야 하는 부분도 있을 것이다. 이를 위해서 산업계, 학계와 협력하여 R&D와 혁신을 이끌어내는 조화로운 접근이 필요할 것이다. **우리는 2025년까지 다음과 같은 성과를 이룰 것이다:**

133. 영국의 사이버 강국 부상에 가장 핵심적인 기술분야에서 연구 결과를 혁신과 새로운 기업으로 전환하는 데 성공하고 있다. 영국 전역의 학자들이 산업 파트너들과 협력하여 보다 진취적으로 연구를 상업화하고 운영할 수 있도록 지원할 것이다. 이를 통해 가장 잠재력 있는 아이디어를 발굴하여 적극적으로 투자 유치를 할 것이다. 영국은 쉽게 모방할 수 없는 공고한 우위를 확보하기 위해 혁신 전략에서 제시한 접근 방식을 기반으로 핵심 기술들의 확고한 생태계 개발을 지원할 것이다.

134. 영국은 마이크로프로세서 보안 설계분야에서 세계 선두주자로서 입지를 더욱 더 공고히 하고 있다.[26] 이는 소프트웨어 보안을 강화하는 신기술을 적용한 컴퓨터 칩을 개발한 Digital Security by Design 프로그램을 기반으로 할 것이다. 이 경험을 인공지능 프로세서에 접목하여 영국 기업들이 세계 시장에서 우위를 선점할 수 있게 할 것이다. 이 기술우위를 확고히 하기 위해 국가 양자 기술프로그램과 협력하여 양자 컴퓨터 안보 모델을 설계할 것이다.

135. 영국은 핵심 산업 통제 시스템, 운영 기술 보안과 이를 자국내에서 시험하고 운용할 수 있는 세계 선도적 기술을 가지고 있다고 알려져 있다. 산학 파트너쉽으로 운영기술 안보 국가 연구소를 설립할 것이다. 세계 최고 연구 프로그램을 진행하고 정부, 군사, 산업 및 국제 파트너들이 이를 영국 내에서 시험 운용해볼 수 있는 장을 제공할 것이다. 그리고 5G 통신 공급망 다양화 전략에서 명시했듯이 영국은 UK Telecoms Lab을 설립하여 정부와 규제기관들이 기업들과 협력하여 새로운 통신 보안체계를 완성하고 영국공급망에서 통신 장비 판매기업들의 다양성을 증가시킬 것이다.[27]

136. 정부는 적대적 행위로 부터 핵심 사이버 기술의 영국의 혁신과 지적 재산을 보호하여 첨단 경쟁력을 유지할 수 있다.[28] 국가안보투자법 2021 목표에 맞춰 외국인 직접 투자 리스크에 대한 자문을 제공하고 기술발전에 따른 안보분야의 기술 리더쉽을 제공할 수 있는 자원과 전문성에 투자할 것이다. 지속적인 산학 협력을 통해 핵심 분야의 R&D를 위한 안전한 환경을 조성하고 지적 재산과 데이터 도용 방지를 위한 강력한 대책을 개발할 것이다.

[26] Microprocessors are the brains of many of the devices we use today. They are ubiquitous, including in critical areas such as telecoms, defence, healthcare and across our major industries. Technological advances in systems design are currently held back by security and safety concerns, which are magnified by increasing system complexity.
[27] DCMS, 5G Supply Chain Diversification Strategy (2020)
[28] With a particular focus on those sectors identified in the National Security and Investment Act 2021: advanced robotics, artificial intelligence, communications, computing hardware, cryptographic authentication, and quantum technologies

디지털 보안 설계

현재 사이버 보안 취약점의 70%는 1970년대 부터 알려진 마이크로프로세서 설계 방식의 결함 때문이다. 이러한 마이크로프로세서는 텔레비전부터 통신까지 모든 디지털 장치에 사용된다. 정부는 이를 시정하기 위해 기술 업계와 협력해왔고 2025년까지 스마트폰과 급증하는 관련 기기들에 사용할 새로운 마이크로프로세서를 출시할 것이다.

마이크로프로세서의 설계를 변경하려면 글로벌 파트너십과 투자가 필요하다. 영국의 리더십과 정부의 7,000만 파운드의 투자로 새로운 미래 기기에 알맞은 보안 장치가 설계 되고 있어 사이버 공격 위협은 급격히 감소할 것이다.

이 판도를 바꾸는 신기술은 영국에서 연구 개발되었다. 마이크로소프트, 구글을 포함한 기술 선도 기업들은 그들의 제품에 이 새로운 보안 기술을 접목하기 위해 투자하고 있다. 영국 전역 대학의 연구원들은 이 보안 기술을 더 효율적으로 사용할 방안을 연구하고 있으며 정부는 영국 중소기업들이 이 새로운 보안이 내장된 제품의 새로운 시장을 찾을 수 있도록 지원하고 있다.

Phil Wilson, Director, Research & Development at The Hut Group
헛 그룹 연구소장

헛 그룹은 빠르게 변화하는 소비재 중심 전자상거래 기업이다. 공통 플랫폼에서 200개 이상의 웹 사이트들이 분당 최대 3000건의 주문을 처리할 수 있고 플랫폼과 고객의 보안이 최우선이다. 당사는 모든 사이버 공격을 억제하기 위해 막대한 노력을 기울이고 있으며, 이러한 이유로 당사 시스템에 "설계에 의한 디지털 보안" DSbD(Digital Security by Design) 기술을 사용할 수 있다는 가능성에 매우 흥분하고 있다. 1억 8천만 파운드의 정부-산업 파트너십을 통해 개발된 이러한 새로운 마이크로프로세서에서 시스템을 구동하면 시스템 복원력이 향상될 것이다. 하지만 복잡한 변화과정 때문에 성능 요구사항을 충족하지 않는 한 새로운 기술을 채택할 수 없다. DSbD 프로그램의 첫 번째 시범 프로젝트가 되는 것은 특권이었고 우리는 가까운 미래에 헛그룹 모든 시스템에 이 새로운 보안기술이 적용되길 희망한다.

목표 2a:
가장 유능한 적들의 위협을 포함한 최고 수준의 위험요소를 적절히 완화하고 영국정부 고객, 파트너 및 동맹국의 요구사항을 충족시키는 강력하고 탄력적인 국가 암호 키 기업 보호

137. 암호 키(Crypt-Key)는 가장 유능한 적의 공격으로부터 영국 정부, 군을 포함한 국가 안보 공동체가 의존하는 핵심 정보와 서비스를 보호하기 위한 암호법 사용을 의미하는 용어 이다. 이는 국가 안보, 국방 역량을 어떻게 배치할지 결정하는 우리의 능력을 뒷받침한다. 세계 최고의 암호키 국가가 되기 위해서는 정부 및 민간 부문에서 최고의 기술이 필요하다.

138. 영국이 미래에도 암호키 주권을 개발할 수 있는 세계 몇 안 되는 국가 지위를 유지할 수 있도록 국내 암호키 산업과 협력하고 정부 역량에 지속적으로 투자할 것이다. 또한 핵심 소재의 공급자로 NATO를 지원하고 암호키 분야의 세계적 리더쉽을 유지 활용할 것이다. 이러한 리더십은 영국내의 고도로 숙련된 산업을 유지하고 최고 수준의 복원력을 자랑하는 엔지니어링분야에서 영국의 강점을 유지하고 핵심 국가 기반시설과 같이 고도의 보안을 요구하는 분야에 필요한 새로운 강력한 역량의 잠재적 개발과 같은 추가 이익을 동반 할 것이다. 핵심국가 기반 시설과 같은 고도의 보증 맥락에서 새로운 강력한 기능을 가능하게 할 수 있는 잠재력을 가지고 있다. **우리는 2025년까지 다음과 같은 성과를 이룰 것이다:**

139. 보다 지속가능하고 세계 최고 산업기반을 갖춘 탄력적이고 안정적인 영국 암호키 기업, 영국이 필요로 하는 모든 종류의 솔루션을 공급하고 선택된 파트너 및 동맹국에 수출. 정부와 산업계의 역량과 전문성을 더욱 효과적으로 결합하고, 기업 관리에 있어 보다 엄격한 국가적인 접근 방식을 채택할 것이다. 이를 통해 영국이 필요로 하는 차별화되고 전문적인 기술 개발을 확보할 것이다.

140. 영국 국내와 동맹국들의 진화하는 요구를 충족하고 영국이 암호키개발 선두 지위를 유지하기 위해 정부 내 더욱 더 강력한 암호키 역량과 서비스를 확보하고 있다. 상품, 시스템 보증과 주요 소재 공급 같은 핵심 서비스를 개선하고 사용자의 요구사항을 이해하기 위해 강력한 기술 리더쉽을 제공할 것이다. 또한 새로운 기술을 활용하여 암호키 서비스를 더욱 보이지 않고 유연해지도록 변형할 것 이다.

141. 영국은 암호키 분야에서 글로벌 리더십을 선도하고, 파트너와 동맹국에 대한 수출을 확대해 왔다. Five Eyes, NATO 및 국제 파트너십에서 영국의 리더십 역할을 유지하고 영국의 암호키 솔루션이 상호 운용될 수 있도록 국제적으로 공인된 표준의 개발을 구체화할 것이다. 그리고 수출 기회를 극대화 하기 위해 업계와 협력할 것이다.

목표 3:
차세대 연결 기술 확보, 글로벌 시장 의존으로 인한 사이버 안보 위험 완화 및 영국 사용자들을 위한 공급의 다양성과 신뢰성 확보

142. 향후 10년 동안 컴퓨팅 파워, 인터넷 연결성 및 자동화는 사물, 시회 기반시설, 장기적으로 인간 자신을 포함한 우리의 환경에, 점점 더 많은 비중을 차지하게 될 것이다. 이것은 사이버 공간의 범위를 확장하고 생성되는 데이터의 양을 크게 증가시킬 것이다. 데이터를 확실하고 안전하게 관리하는 능력이 우리 경제의 안정적 운영에 핵심이 될 것이다.

143. 가능한 모든 차세대 연결 기술이 안보와 복원력을 중심으로 설계, 개발 및 배치되고, '설계로 안전하게' 접근 방식을 수용하기 위해 확실하게 다같이 노력해야 한다. 기술 공급망의 글로벌 특성은 기술 의존성이 초래하는 위험을 보다 적극적으로 관리하기 위해 가용할 수 있는 모든 수단을 동원해야 한다는 것이다. 가능한 안보 보장과 확보를 위해 노력하고 불가능한 경우 국내 규제 및 표준에 대한 국제 협력을 포함한 위험 요소 완화를 위한 강력한 조치를 시행할 것입니다. **우리는 2025년까지 다음과 같은 성과를 이룰 것이다:**

144. 영국 전역에서 판매되는 소비자 연결 상품은 필수 사이버 보안 표준 준수. 영국에서 판매되는 모든 새로운 소비자 연결 상품은 최소 보안 표준을 시행할 수 있도록 상품 보안 및 통신 기간 산업 법안을 도입하고 시행할 것이다. 스마트 전기차 충전포인트, 에너지 스마트 가전 등 스마트하고 유연한 에너지 시스템으로 사이버 보안 전환을 지원할 것이다. 우리는 기술 표준에 대한 글로벌 합의를 도출해내기 위해 표준 기관, 업계 및 국제 파트너들과 협력할 것이다. 또한 새로운 보안 지침을 포함하여 영국 기관들이 좀 더 안정적인 방식으로 통신 기기를 조달, 배치, 관리할 수 있도록 지원할 것이다.

146. 클라우드, 소프트웨어, 관리형 서비스 및 앱 스토어와 같은 주요 디지털 서비스 제공 업체는 사이버 보안 표준을 준수해야 한다. 이 사이버 보안 표준은 사이버 위협으로 부터 기관과 소비자를 보호할 수 있다. 디지털 서비스 제공자에 대한 기존 규제를 강화·확대하고 ICO 역량을 강화하여 디지털 제공자가 서비스와 관련된 리스크를 보다 적극적으로 관리할 수 있도록 할 것이다. 주요 기술 기업을 포함한 산업과 지속적으로 협력하여 시장 전문성을 활용하고 영국의 디지털 공급망을 확보하는 데 모두가 역할을 할 수 있도록 할 것이다. 그리고 디지털 공급 업체를 중심으로 한 정책 솔루션 개발을 주도할 것이다.

146. 시민과 기업의 이익을 위해 **영국은 안전하고 지속 가능한 공간 연결 기술 채택에 앞장서고 있다.** 스마트 시티로도 알려진 연결된 장소(Connected place)들은 교통 관리, 오염 감소, 그리고 돈과 자원 절약과 같은 실질적인 이익을 사회에 제공할 수 있는 잠재력을 가지고 있다. 그러나 이렇게 보다 효율적인 기능을 제공하는 상호 연결성은 사이버 위협에 취약하고 잠재적인 사이버 공격 대상이 된다. 연결된 장소들에 대한 NCSC의 보안 원칙을 바탕으로 기업, 인프라, 공공부문 및 시민들에게 미치는 위험을 줄여 나갈 것이다.[29] 지방 자치단체와 항만, 대학, 병원과 같은 기관들의 역량을 강화해서 연결된 장소 (connected place) 기술을 안전하게 구입해 사용할 수 있게 할 것이다. 또한 연결된 장소들의 안보에 대한 일관되고 효율적인 접근을 위한 국제적인 합의를 도출할 것입니다.

147. 사이버 안보는 영국에 들어온 다른 신 기술에도 적용되도록 설계되었다. 영국은 사이버 안보 위험을 야기할 수 있는 신흥 기술 응용 프로그램을 식별하고, 이러한 기술의 안전하고 안정적인 개발을 선도해 나갈 것이다. 정부가 디지털 트윈과 광범위한 '사이버 물리적인 기간 산업' 기술에서 영국 역량을 위한 옵션을 검토함에 따라 사이버 안보가 의사 결정의 핵심이 되도록 할 것이다.[30] 그리고 광범위하게 연결되고 자동화된 차량 개발에 있어 현재 영국의 선도적인 위치를 보장하기 위한 계획을 발표할 것이다.[31]

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

Shadi A. Razak, CTO and co-founder of Angoka
앙고카의 최고기술자이며 공동 창업자

정부의 안전한 연결 도시(커넥티드 플레이스) 지침 발간과 자율주행차 이용 증가로 우리 사회의 보안의 중요성이 대두 되고 있다. 앙고카는 NCSC 사이버 육성 가속화 프로그램의 자랑스러운 졸업생이다. 국가 핵심 기간 산업에서 육지 항공 이동성 등에 이르기까지 광범위한 애플리케이션에 대한 솔루션을 제공하여 끝에서 끝까지 보안성과 복원력을 확실히 제공한다.

앙고카의 목표는 연결된 장치와 기계 간 통신의 네트워크에 점점 더 복잡하고 의존하게 되는 스마트 시티와 모빌리티의 안전과 복원력을 보장하는 것이다. 우리의 솔루션은 역학적인 업데이트를 통해 공격자에게 항상 목표가 움직이도록 하고 분산형 양자 방지 보안을 운영하는 신뢰할 수 있는 영역을 만들어 낸다. 즉, 기기 소유자가 보안을 완전히 제어할 수 있다.

Angoka Team demonstrating their solution

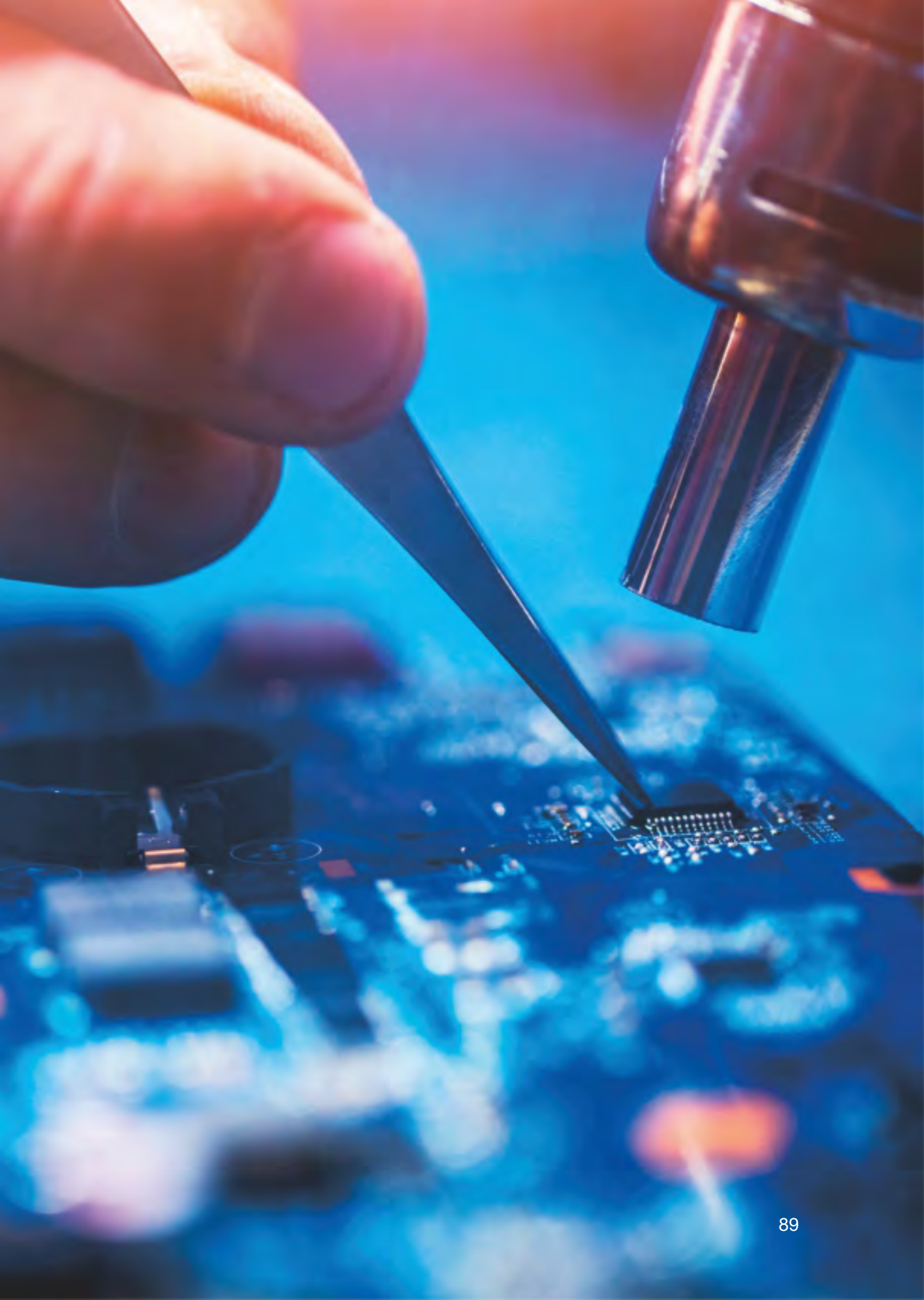
목표 4:
우리의 민주주의 가치 추구, 사이버 안보 보장, 과학 기술을 통한 영국의 전략적 이익 증진을 위해 가장 중요한 우선 순위인 글로벌 디지털 기술 표준 개발을 다중 이해 당사자들과 협력하여 추진한다.

148. 글로벌 디지털 기술 표준은 인터넷, 통신 네트워크 및 신흥 기술 기능의 핵심이다. 어떻게 개발되고 배치되는가는 우리의 사이버 안보 목표, 경제적 번영, 그리고 우리의 규범과 가치에 영향을 미칠 수 있다. 역사적으로 이러한 표준은 시장 지배력이 가장 높은 세력이 주도하고 중소기업, 학계, 기타 전문가를 포함한 일부 중요한 이해당사자들이 참여할 수 없는 물리적인 진입 장벽이 존재했다. **우리는 2025년까지 다음과 같은 성과를 이룰 것이다:**

149. 글로벌 디지털 기술 표준 생태계에 다자간 참여 확대. 우리는 주요 표준 개발 기구에 다중이해당사자 참여를 강화하고 국제 전기 통신 연합 대표단과 함께 선도적 역할을 할 것이다. 유엔 인터넷 거버넌스 포럼 등을 통해 정책 입안자들의 주요 동향과 고려사항에 대한 공개토론을 추진할 것이다. 또한 영국의 G7 의장국 임기 동안 설립된 디지털 표준 연락 그룹과 같은 국제 파트너들과의 정보 공유와 조율 기능을 강화할 것이다.

150. 민주주의 가치, 사이버 안보 고려사항, 신흥 기술에 대한 영국의 연구와 혁신으로 보다 효율적으로 정해진 영국의 우선 순위 영역에서의 글로벌 디지털 기술 표준. 인터넷 프로토콜, 미래 네트워크, 인공지능(AI) 등의 분야에서 산·학·기술 전문가 및 시민사회와 협력해 기술표준 개발에 있어 중요한 공공정책 고려사항에 대한 인식을 높일 것이다. 국가 AI 전략에서 명시한 대로 AI 표준화에 대한 영국의 글로벌 참여를 지원하기 위해 AI 표준 거점을 시범 운영할 것이다.

151. 이 모든 것은 정부, 영국표준협회 (BSI), 영국 국립물리연구소 (National Physical Laboratory) 간의 국가 AI 전략에서 제시된 이니셔티브와 같이 영국 내 전략적 조정 메커니즘에 의해 뒷받침될 것이다. 또한 혁신, 성장, 평준화를 가능케하는 표준을 촉진함으로써 영국의 번영을 지원할 것이다.



전략 축 4:

글로벌 리더십

국제 질서 안정과 번영을 위한 영국의 글로벌 리더십과 영향력 향상

152. 자유롭고 개방적이며 평화롭고 안전한 사이버 공간은 우리의 집단 안보와 번영에 여전히 중요하며, 국제적인 참여는 영국의 모든 사이버 전략 목표를 달성하기 위해 필수적일 것이다. 하지만, 시스템 경쟁 시대에 대응하기 위해, 영국은 이제 사이버 공간에서 우리의 이익과 가치를 증진시키기 위해 좀 더 적극적인 국제 리더십 역할을 맡을 것이다. 사이버 공간에서 영국의 활동과 사이버 전문 지식은 정부의 광범위한 외교 정책 의제를 실행하는 데 중심에 놓일 것이다: 우리는 이를 개방적이고, 안전하고, 번영하는 국제 질서를 달성하기 위해 적극 활용할 것이다.

153. 영국은 핵심 동맹을 강화하고 동시에 문제 해결, 부담 분담 국가로서 산업, 글로벌 기술 표준 기구, 시민 사회 및 학계 등 광범위한 파트너들과 협력할 것이다. 또한 아프리카와 인도-태평양의 파트너들과의 심도 깊은 관계 발전에 투자하여 보다 새롭고 유연한 동맹의 기회를 잡을 것이다. 외교 수단 강화, 해외 영향력과 국내 강점 연결, 운영 및 전략 커뮤니케이션 전문 지식, 기술 프로그램 과 경제적 파트너십을 선의를 위한 글로벌 세력으로서 활용하여 영국의 외교 수단을 지속적으로 강화할 것이다. 우리의 접근 방식은 자신만을 위한 것이 아니라 세계 안보와 번영을 위한 것이다.

목표 1:
국제 파트너의 사이버 복원력과 안보 강화 및 적대국 방해와 억지를 위한 집단 행동 확대

154. 집단 행동과 상호 복원력은 업스트림 위협 대처에 있어 핵심 개념이다. 또한 사이버 위협 행위자들이 영국과 그 파트너에 대한 공격을 감행할 동기를 감소시킨다. **우리는 2025년까지 다음을 이룰 것이다:**

155. 영국의 국제파트너들은 복원력 구축, 사이버 위협을 조사하고 파괴하는 시스템, 정치적 결의, 거버넌스와 같은 훌륭한 역량이 있다. 이는 영국 시민들에 대한 해외로부터의 사이버 위협을 감소시킬 것이다. 우리는 동유럽, 아프리카, 인도-태평양에서 사이버 역량 구축 지원에 우선 순위를 두고, 중동 및 미주 지역의 핵심 동맹국들과 지속적으로 협력할 것입니다. 영국 산업계와 학계에 관심을 불러 일으키고, 법 집행과 국방 전문지식에 대한 더 많은 투자를 해서 보다 통합된 정부 전체의 기술 제안을 개발할 것이다. 영국 정책의 주안점은 핵심 국제 공급망과 기반 산업을 보호하고, 디지털 기술의 안전한 사용을 증진하고, 이를 위해 업계 파트너들과 본격적으로 협력하는 것이다.

156. 또한 시민사회 조직의 역량 강화를 위해 더 많은 일을 할 것이며, 기술과 사회를 둘러싼 가치 중심 토론을 활성화하고, 지역 책임 메커니즘을 구축할 것입니다. 그리고 UN, 파이브 아이즈, NATO, G7, EU, 영연방, OECD, 사이버 전문지식에 관한 글로벌 포럼 (GFCE), 아세안 포럼, 아프리카 연합과 세계은행을 포함한 효율적인 다자기구들과 지속적으로 협력할 것이다.

157. 영국의 이익, 해외 시민 보호 증진을 위해 해당 지역에 맞춤 설계한 국제 사이버 위생 캠페인을 개발하고 영국 해외공관들과 함께 진행할 것이다. 이 캠페인의 목적은 해킹, 데이터 및 IP 도용, 랜섬웨어 등과 같은 악성 활동의 비용을 높이는 것이다. 외교관, 현지공관직원, 영국 비즈니스 커뮤니티 및 해외 원조 개발 활동가들이 이 캠페인을 진행할 것이다.

158. 영국의 적들에게 심각한 결과를 초래할 역량이 되고 의지도 있는 광범위한 국제 동맹. 영국은 더 적극적인 외교활동, 연합작전, 정보 공유를 통해 국제적인 결의와 역량을 향상시킬 것이다. 정책, 운영 및 법 집행 채널을 통한 종합적인 접근과 공격 목표 맞춤형 사이버 제재, 사이버 위협 행위자의 위협, 공격 비용 인상을 초래하는 수단을 강구하여 대응 효과를 증진시킬 것이다. 주요 동맹국과 파트너국의 사이버 역량 전반에 걸쳐 상호 이해를 증진시키고, 사이버 운영을 동맹국들의 육, 해, 공, 사이버, 모든 영역에서 운영에 통합할 것이다.

159. 그리고 영국과 일부 동맹국들이 각각의 사이버 주권 사항을 자발적으로 NATO에 제공하여 NATO 작전과 임무에 통합하는 프로세스와 같이 집단 행동 강화를 위한 NATO 동맹의 사이버 안보 역량 개발을 지속적으로 지원할 것이다.

목표 2:
자유롭고 개방적이며 평화롭고 안전한 사이버 공간 확보를 위한 글로벌 거버넌스 형성

160. 영국의 가치를 공유하지 않는 국가들은 안보를 빙자하여 사이버 공간에 대한 그들의 권위주의적 비전을 추진하기 위해 자유롭고 개방적인 인터넷의 문제점을 악용한다. 영국은 우리의 민주주의 가치에 맞춰 국제 제도와 규칙이 발전하도록 동맹국, 파트너들과 보다 적극적으로 협력할 것이다. 영국과 세계 경제 성장을 지원하고, 집단 안보를 강화하며, 공격적인 사이버 수단의 책임 있는 사용을 장려하고, 악의적이고 무책임한 활동에 대해 실질적인 책임을 추궁하는 것을 목표로 한다. 우리는 2025년까지 다음과 같은 성과를 이룰 것이다:

161. 사이버 공간과 인터넷의 글로벌 거버넌스는 영국의 이익과 가치를 보호하고, 영국과 그 파트너들은 국제 거버넌스 및 표준 체계의 개발과 실행에 영향력을 증대할 것이다. 우리는 세계 경제 성장과 안보 증진을 위해 사이버 공간을 규율 체계 형성을 위해 좀 더 진보적이고 능동적인 접근을 할 것이다. 사이버공간에서 규칙, 규범, 원칙 적용에 대한 국제적인 논의를 이끌고 파괴적이고 불안정한 행위를 효율적으로 억제하기 위해 단계적이고 실용적인 대책을 마련, 이행할 것이다. OSCE, 아세안, GFCE과 같은 주요 지역 및 전문기구를 통해 이를 수행하고 국제 협력, 인권 보호 강화를 위해 부다페스트 협약과 함께 새로운 국제 사이버 범죄 조약을 개발하기 위한 UN 프로세스에 건설적으로 참여할 것이다.

162. 또한 사이버 범죄에 관한 부다페스트 협약을 계속 지지하며, 국제적인 파트너들과 협력하여 이 협약이 최상의 국제 합의로 남을 수 있도록 강력한 사례를 만들어 갈 것이다. 또한 인터넷 주소 관리 기구와 인터넷 거버넌스 포럼(IGF)을 포함한 인터넷 거버넌스를 위한 다자간 프로세스를 지속적으로 추진하고 강화해 나갈 것이다. 이러한 노력은 글로벌 디지털 기술 표준(기술 장에 기술됨)을 구체화하고 영국 사이버 안보 수출 확대(아래 설명)로 보완될 것이며, 영국 표준을 다른 국가의 사이버 생태계에 적용, 확립하는 데도 도움이 될 것이다.

163. 대부분의 '중립' 국가들은 사이버 공간과 인터넷의 미래에 대한 영국의 비전을 지지하고, 다중 이해당사자 체제에 대한 독재 국가들의 영향에 더 성공적으로 대항한다. 독재적인 접근법 없이도 사이버 공간의 문제를 해결하고 혁신, 발전, 성장이 가능하다는 것을 보여줄 것이다. 우리는 디지털화로 고민하는 국가들이 국제 논의에 참여하고 합의된 프레임워크를 구현하는 데 필요한 모든 범위의 법적 및 전략적 커뮤니케이션 전문지식을 구축하도록 지원할 것이다. 사이버 능력의 무책임한 사용을 지속적으로 폭로하여 국제적인 신뢰를 쌓을 것이다. 그리고 우리의 공격적 사이버 기능을 활용할 수 있는 모든 곳에서 개방적이고 투명한 방식으로 접근하여 선을 위해 행동하는 영국의 명성을 강화할 것이다.

목표 3:
영국의 사이버 역량과 전문 지식을 활용하여 전략적 우위를 강화하고 폭넓은 외교 정책과 경제번영을 추구한다.

164. 시스템 경쟁과 급속한 기술 변화에 대응하여, 영국의 사이버 활동과 능력은 영국의 전략적 우위를 강화하고 외교 정책과 번영 목표를 추진하기 위한 국가 능력과 자원의 일환이다. 우리의 목표는 세계의 개방 사회, 경제 번영, 인권 수호와 영국 번영을 동시에 견인하는 국제 질서를 확립하는 것이다. **우리는 2025년까지 다음과 같은 성과를 이룰 것이다:**

165. 사이버 공간에서 그리고 사이버 공간과 관련된 우리의 활동은 글로벌 안정성을 향상시켰고, 훼손되고 있는 규칙에 기반한 국제 시스템, 개방 사회와 민주주의를 보호했다. 우리는 사이버공간의 디자인, 개발, 이용에 있어 인권, 다양성, 양성평등을 수호하기 위한 국제 가치에 기반한 캠페인을 전개할 것이다. 여기에는 인터넷 차단, 편향된 인공지능 알고리즘 방지, 온라인 안전 증진을 포함되지만 꼭 이에 국한되는 건 아니다. 우리는 6개 대륙에 전역에 뻗어 있는 사이버 정책 네트워크에 더욱 투자하여 민주적 가치, 시스템, 프로세스를 보호하고 규칙 기반의 국제 시스템(유엔, 세계보건기구, 글로벌 무역 시스템 포함)을 강화하기 위해 더욱 효율적으로 경쟁할 것이다. 우리는 전략적 커뮤니케이션의 사용을 강화하여 영국의 연구 협업과 학술 교류 프로그램을 증진하고 영국의 아이디어가 실제 적용 될 수 있도록 할 것이다.

166. 영국은 사이버 솔루션 및 사이버 전문지식 세계 3대 수출국 중 하나로, 영국 사이버 산업은 해외 정부 및 주요 기업 고객에게 사이버 안보 솔루션 '고투' 제공국으로 평가받고 있다. 영국 사이버 안보 대사 프로그램 및 국제 네트워크의 후원으로 보다 적극적인 국제 정부 대 정부 참여를 통해 영국 사이버 안보의 최고 수준을 보여줄 것이다. 영국 전역의 기업들이 투자를 유치하고 수출 경쟁력 있는 갖출 수 있도록 혁신의 모든 단계가 수출의 활주로가 될 수 있게 지원할 것이다. 새로운 '수출 교육진'을 통해 중소기업에 더욱 많은 지원을 제공할 것이다.[32, 33] '사이버 성장 파트너십'과 '영국 사이버 생태계 헌장'에 명시된 여러 노력과 함께, 우리는 새로운 '사이버 역량 캠페인 사무소'를 개발하여 주요 수출 캠페인에 보다 체계적이고 조화로운 지원을 제공할 것이다.

[32] Described in the UK Innovation Strategy (2021)
[33] The UK Defence & Security Exports (UKDSE) Export Faculty is an online learning and development hub aimed at SMEs in the defence and security sector with specific modules for cyber security companies. Registering for the Faculty provides access to a programme of curriculum based learning modules and in addition, valuable information around UK Defence and Security Exports planned events and activities.

Charles Juma, UK Digital Access Programme in Nairobi
나이로비 영국 디지털 접근 프로그램

내 이름은 찰스 주마이다. 케냐에서 글로벌, 범 정부 영국 디지털 접근 프로그램의 일환으로 사이버 안보, 디지털 개발, 포용 및 기업가정신을 구체화시켜 그 실행을 주도한다. 또한 분쟁안정안전기금(CSSF) 사이버 포트폴리오에 따른 보완 프로젝트를 지원한다. 온라인 안전, 보안, 데이터 보호 및 사이버 공간의 책임 있는 이용의 중요성은 아무리 강조해도 지나치지 않는다. 우리가 COVID-19 대유행에서 배웠듯이, 온라인 안전 및 위생은 공중 보건 및 위생만큼 중요할 수 있다. 영국 정부 사이버 파워 일원으로 온라인상의 위협과 피해로부터 모든 사람들이 보호받을 수 있도록 나의 열정을 쏟아 부을 것이다.

Sara Merchant, Cyber Officer at the British Embassy, Tbilisi
트비리시 영국 대사관 사이버 담당관

나는 트비리시 영국 대사관에 사이버 담당관으로 파견되었다. 조지아 정부 및 NCSC UK와 긴밀히 협력하고 있다. 기본 업무는 정치 에서부터 새로운 사이버 전략의 실행을 지원하고 조지아의 기술 역량 증진을 위해 영국 전문가들을 활용하는 것이다. 조지아가 사이버 위협에 대한 복원력을 기를 수 있도록 영국의 전문지식을 지원하는 일을 주도하게 되어 영광스럽다. 불행하게도 적대적인 국가 활동의 최첨단에 서서 많은 경험을 가진 나라로서 영국은 이곳 조지아에서 배울 것이 많다. 우리의 일은 우리를 더 강하고, 회복력 있고, 더 잘 이해할 수 있게 해준다.

전략 축 5:

위협에의 대응

영국의 안보 강화를 위한 사이버 공간에서 그리고 사이버 공간을 통해 적 탐지, 방해 및 억지

167. 우리가 직면한 위협의 본질은 복잡하다. 사이버 공간에서의 위협(예: 온라인 활동에 대한), 사이버 공간을 통한 영국과 파트너국에 대한 위협(예: 네트워크로 연결된 영국의 핵심 국가 기반 시설에), 그리고 국제 사이버 기반 시설의 주요 기능에 대한 위협이 걱정된다. 이 모든 위협은 사람들이 의존하고는 서비스의 가용성 또는 이러한 시스템 내의 데이터와 정보의 기밀성 또는 보존에 영향을 미칠 수 있다. 위협에 대처하는 기본은 이 문서의 앞부분에서 와 제시한 바와 같이 사이버 복원력을 증진하는 데 있다. 이 장에서는 우리가 사이버 공간에서 영국을 공격하는 비용과 위험을 높이고 사이버 강국으로서 우리의 잠재력을 최대로 발휘할 수 있는 방법에 초점을 맞출 것이다.

168. 국가 사이버 안보전략 2016-2021 이후, 우리는 위협을 완화하기 위한 접근 방식을 전환해 왔습니다. 우리는 국가 사이버안보센터(NCSC)의 일환으로 세계 수준의 사이버 위협 탐지 및 분석 역량을 구축했다. NCSC는 국내외 공공 및 민간 부문의 파트너와 협력하여 위협과 사고를 탐지하고 대응한다. 또한 NCSC는 광범위한 정보 커뮤니티의 일환으로 정책 입안자들에게 사이버 위협을 억지하는 우리의 핵심 접근법인 영국의 이익을 침해하는 공격의 속성을 알릴 수 있었다. 국가 공세 사이버 프로그램과 새로운 국가사이버군(NCF)을 통해 우리의 공격적 사이버 역량에 상당한 투자를 해왔다. 또한 통합된 국가범죄청(NCA) 주도로 국가차원의 법 집행 대응을 개발하고 사이버 공간에서 적대적 범죄 행위에 대한 대가를 높이고 그 행위를 방해하기 위해 노력해 왔다. 우리는 공공 부문과 민간 부문에서 결과적인 통찰력을 영향력 있는 완화로 변환하는 수단을 통해 세계수준의 위협 탐지 및 평가 기능을 개발했다. 그리고 우리는 적대 행위자들에게 비용을 부과하기 위한 또 다른 수단으로 자율적인 사이버 제재 체제를 개발했다. 외교적 개입과 더불어, NCSC, 보안 및 정보 기관, NCA, 광범위한 법 집행 기관 및 NCF는 적에 직접 대응하고 공격을 방지하고 피해를 줄이기 위한 조치를 취함으로써 위협으로 인한 실제 영향을 줄였다.

169. 그러나 위협은 더욱 정교해지고 복잡해지고 심각 해졌다; 그리고 우리의 노력은 계속해서 영국과 영국의 이익을 성공적으로 목표로 하는 공격자들의 위험 계산을 아직 근본적으로 바꾸지 않았다. 영국에 대한 사이버 공격은 간첩 행위, 범죄, 상업적, 재정적, 정치적 이익, 파괴 및 허위 정보 확산을 목표로 한다. 공격자는 위협 완화를 피하는 기능을 개발한다; 점점 더 정교해지는 사이버 수단과 관련 조력자들은 성장산업에서 상품화되어 모든 유형의 악의적인 행위자의 진입 장벽을 낮추고 있다. 그리고 중요한 데이터를 도용하고 암호화하고 랜섬웨어 지불을 갈취하는 행위자의 능력이 계속 증가하여 기업과 주요 공공 서비스를 중단시키면서 이에 대한 보상이 증가하고 있다. 그 결과 공격자는 점점 더 많은 재정적 이익을 취하고, 사생활과 언론의 자유를 악용하며, 허위 정보를 통해 사건 조작을 시도하고 있다.

170. 따라서 영국의 접근 방식은 이제 우리의 적들에게 대가를 치르게 하고, 가해자들을 추적하고, 방해하며, 미래의 공격을 억지하기 위해 모든 범위의 수단과 능력을 일상적이고 통합적이며 창의적으로 사용하는 통합적이고 지속적인 캠페인 기반으로 전환될 것이다. **이 접근법의 핵심 지원 요소는 다음과 같다:**

- NCF의 지속적인 발전 - 적국에 대한 공격적 사이버 작전을 수행하기 위한 영국의 다음 단계 역량

- 영국에 대한 위협에 대처하기 위한 맞춤형 범정부 캠페인 - 외교, 군사, 정보, 법 집행, 경제, 법률 및 전략 커뮤니케이션 수단 활용

- 우리의 적들에 대해 기술적 우위를 유지할 수 있도록 하기 위한 새로운 투자 - 법 집행 기관이 필요한 규모와 속도로 수사를 추진할 수 있고, 중범죄자와 이들이 의존하는 서비스를 예방하고 탐지하기 위함

- 정부 및 산업 전반에 걸친 데이터 공유의 업그레이드 – '복원력' 장에서 제시

171. 사이버 공간은 영국에게 기회를 제시하며, 우리의 국익을 적극적으로 추구할 수 있는 새로운 방법을 만들어낸다. 예를 들어, 공격적 사이버 작전은 유연하고 확장 가능하며 비확산할 수 있는 다양한 조치를 제공하여 영국이 전략적 우위를 유지하고 국가 우선순위를 실행할 수 있게 하며 이는 개개인이 실질적 상해를 입을 위험을 피할 수 있는 방법으로 진행된다.

172. 우리는 NCF를 통해 지속적으로 우리의 공격적 사이버 역량을 개발하고 투자할 것이다. NCF는 국가와 국민, 그리고 우리의 삶의 방식을 보호하기 위해 사이버 공간과 현실 세계에서 적들과 경쟁할 수 있는 영국의 능력을 변화시킬 것이다. 이러한 능력은 외교적, 경제적, 형사적 정의, 군사적 힘의 지렛대와 함께 선의의 힘으로 책임감 있게 사용될 것이다. 그들은 국가 안보, 경제적 복지와 관련된 광범위한 정부 우선순위를 지원하고 발전시키고 중범죄를 예방하고 탐지하는 데 사용될 것이다.

목표 1:
영국, 영국의 이익 및 국민을 보호하기 위해 국가, 범죄자 및 기타 악의적인 사이버 행위자와 행위에 대한 정보를 탐지, 조사 및 공유한다.

173. 우리는 2025년까지 다음과 같은 성과를 이룰 것이다:

174. 정부는 국가, 범죄자 및 기타 악성 사이버 행위자의 사이버 능력과 영국에 대한 전략적 의도를 포괄적으로 이해하고 있다. 2016년 전략에 따라 사이버위협을 이해하기 위해 정보기관과 법 집행기관에 상당한 투자를 해왔고 지속적으로 늘려갈 것이다. 특히 사이버 범죄 위협과 이들의 타국, 다른 국제, 국내 위협과의 연계성, 기술적 가능 요인 등에 대한 법 집행의 이해 및 대처 능력을 증진시켜 보다 효율적인 정책대응 방안을 개발할 것이다. 정보 기관 및 법 집행 기관 전반의 공동 데이터 접근과 활용 전략을 통해 정부 전반의 위협 탐지 조정 방식을 개선할 것이다. 어떻게 개인이 사이버 범죄자가 되고, 이를 방지하는 조치들을 포함하여 우리 적들의 의도와 의사결정 기준, 그리고 우리의 행위가 그들에게 미치는 영향을 이해하는 데 더욱 집중할 것이다.

175. '복원력' 장에서 제시한 사이버 사건과 범죄에 대한 더 빠르고 더 용이한 보고는 이러한 결과를 달성하는 데 도움이 될 것이다.

176. 가장 심각한 국가, 범죄 및 기타 위협을 일상적이고 포괄적으로 조사하여 모든 정보 소스를 활용하고 정부, 법 집행 기관 및 민간 부문에 걸친 전문 지식을 통합한다. 우리는 영국의 법 집행 기관 사이버 네트워크의 정보, 운영 및 기술적 능력을 구축할 것이다. 조직 범죄 집단을 목표로 했던 NCA의 사이버 정보 역량, 영국 전역의 정보 접근과 이동을 강화하는 지역 정보 구축 이니셔티브, 그리고 법 집행 기관이 사이버, 디지털 범죄를 조사하고 방해하는 데 필요한 기술과 역량에 투자할 것이다.

177. 조사는 모든 출처의 정보에 의해 지원되고 기업이 법 집행 기관과 데이터를 보다 쉽게 공유할 수 있도록 지원하는 것을 포함하여 민간 부문 전반에 걸친 기술과 지식을 활용할 것이다. 그리고 사이버 범죄에 대한 경찰 대응의 HMICFRS의 권고를 지속적으로 이행하여 국가와 지역 차원의 사이버 범죄 네트워크가 안전한 기반 위에 유지되도록 할 것이다.[34]

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

178. 위협에 대한 정보와 데이터는 적절한 규모와 속도로 일상적으로 공유되며, 이를 수신한 사람들은 더 많은 조치를 취할 수 있다. NCSC는 위협 정보를 수신하고 공유할 수 있을 뿐만 아니라 집단 이익을 위해 활용할 수 있는 광범위한 분야에 걸쳐 보다 효과적인 네트워크 방어자 커뮤니티를 구축하기 위한 다양한 이니셔티브를 시험해 왔다. 우리는 정부 사이버 조정 센터 (Government Cyber Coordination Centre, '복원력' 장에서 기술)의 지원을 받아 정부가 스스로를 더 잘 방어할 수 있게 지원하는 데 중점을 두고 이 일을 확장할 것이다. 금융권 사이버협력센터가 이미 민간 부문에서 선두를 달리고 있다.[35]

179. NCSC는 또한 새로운 위협을 추적하는 방법을 조사하고 있으며, 특정 유형의 사이버 공격을 탐지하는 데 머신 러닝이 사용될 수 있는지 여부를 탐구하기 위해 앨런 튜링 연구소와 계속 협력하고 있다. 이 연구는 인공지능을 이용하여 악성 활동을 탐지하는 방법에 대한 이해를 지속적으로 향상시킬 것이다.

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

사이버 범죄 방지는 또한 다른 유형의 범죄 행위를 방지한다.

사이버 범죄(컴퓨터 오남용법 위반에 기술)는 컴퓨터, 네트워크, 데이터 및 기타 디지털 장치에 대한 무단 액세스 또는 이러한 범죄를 저지르기 위한 도구의 제작 또는 공급을 유발하는 관련 행위가 있을 때 발생한다. 이를 통해 사이버 범죄자는 랜섬웨어 공격, 무단 계정 접근, 지적 재산권 절도, 서비스 거부 공격, 대규모 개인 정보 세트 도용과 같은 추가로 악의적인 사이버 활동을 저지를 수 있으며 이는 심각하고 범죄이고 증가하고 있다.

시민들에게 사이버 범죄는 종종 그들이 가능하게 하고 촉진시키는 추가적인 범죄에서 나타난다. 무단 컴퓨터 접속은 광범위한 사기, 절도, 성착취로 이어질 수 있으며, 경우에 따라 스토킹, 가정 내 학대와 괴롭힘을 용이하게 할 수 있다. 이 모든 범죄들은 매일 영국 시민들에게 심각한 해를 끼치고, 사업체들을 파괴하고 삶을 망친다. 그러므로 사이버 범죄는 괴롭힘과 학대, 혐오 발언, 허위 정보의 확산, 갱 문화 및 폭력의 조장, 또는 미성년자 음란물 시청과 같은 더 광범위한 온라인 안전 문제와 구별되고 다르다. 정부는 온라인 유해 백서와 온라인 안전 법안 초안을 통해 이러한 문제들을 제기하고 있다.

목표 2:
영국, 영국의 이익 및 국민에 반하는 국가, 범죄자 및 기타 악의적인 사이버 행위자와 활동을 억지와 방해.

180. 우리는 2025년까지 다음과 같은 성과를 이룰 것이다:

181. 국가, 범죄자 및 기타 악의적인 사이버 행위자가 영국을 목표로 삼는 것은 더 많은 비용과 높은 위험을 초래한다. 우리는 악의적이고 범죄적인 사이버 행위자들의 행동에 영향을 미치기 위해 영국의 모든 능력(외교적, 경제적, 은밀한, 공공연한 수단)을 활용하는 맞춤형 억지 캠페인을 지속적으로 시행할 것이다. 특히 제재, 법 집행, NCF 운영 등 심각한 대가를 치르게 할 강력한 역량과 의지를 적대국에 전달하는 방식을 개선할 것이다. 잠재적인 범죄자들에게 수습이나 근무 장소와 같은 더 나은 대안을 제공하기 위해 산학 협력과 NCA의 사이버 선택 프로그램을 통해 개인들이 사이버 범죄에 연루되는 것을 방지할 것이다.

182. 또한 국가 위협이 어떻게 진화했는지 설명해주는 새로운 범죄를 도입하고 기존 법률을 업데이트해서 국가위협대처법을 통해 법 집행 기관 및 정보 기관이 필요로 하는 권한과 수단을 제공할 것이다. 그리고 우리는 사이버 범죄의 수익금을 확인하고, 압수하고, 회수할 수 있는 법 집행의 능력을 최적화하기 위해 2002년 범죄수익법을 개정할 것입니다. 특히 기소할 수 없는 범죄자들로 인한 리스크를 완화하기 위해 시민 몰수권을 만들어 이를 해결할 것이다.

183. 국가, 범죄자 및 기타 악의적인 사이버 행위자들은 영국을 목표로 하기 어려워 질것이다 – 우리의 방해와 그들의 활동 및 능력의 훼손으로 인해 랜섬웨어를 처리하기 위해 정부의 정책과 운영 방식을 검토할 것이며, 이를 우리의 최우선 캠페인으로 채택하고 업계 및 국제 파트너들과 협력할 것이다. 우리는 사이버 공간의 기밀성, 완전성 및 가용성과 사이버 공간의 데이터 및 서비스를 방해하는 위협에 대처하기 위해 NCF, NCSC, NCA 및 광범위한 법 집행 기관, 외교 및 정보 커뮤니티 간의 파트너십을 극대화할 것이다. 특히 사이버 범죄 인프라를 타깃으로 하는 역량에 투자하고, 악성 사이버 행위를 방해하기 위해 우리의 법 집행, 공격 사이버 역량을 전개할 예정이다. 우리의 적들은 사이버 능력을 구축하고 악의적 목적으로 점점 더 많이 사용하고 있다. 우리는 이러한 노력을 방해하고 영국을 방어하고 보호하기 위해 NCF를 적절히 활용할 것이다.

184. 우리는 또한 상업 및 형사 시장을 통해 국가들과 조직 범죄 집단에 대한 첨단 사이버 능력 확산을 막기위해 사이버 범죄를 활성화, 촉진 또는 미화하려는 온라인 플랫폼에 맞서 싸울 것이다.

사이버 범죄자들에 대한 형사 정의 증진 - 영국에서 사이버 범죄자를 기소하는 데 필요한 형사 정의 능력 향상. 컴퓨터 오남용법(CMA)과 관련 권한을 검토해 사법기관이 범죄자의 새로운 위협과 새로운 위협을 수사할 수 있는 능력을 갖출 수 있도록 하고, 늘어나는 사이버 사건을 처리하기 위해 전문 검사를 더 많이 도입할 예정이다. 우리는 또한 국가경찰청장 협의(NPCC)의 사이버능력설명서 및 '경찰대학 사이버 디지털 경력 진로'를 통해 사이버 전문 지식을 갖춘 경찰관이 지속적으로 공급될 수 있도록 전문가, 법 집행 능력, 실행 및 주류화를 개선할 것이다.

Susan Moody, Police Service of Northern Ireland (PSNI) Prevent Officer
북아일랜드 경찰국 예방관

컴퓨터와 모바일 기기들은 젊은 사람들의 일상 생활의 일부이다. 기기들은 엄청난 기회 뿐 아니라 오사용시 위험을 제공한다. PSNI 내의 예방 기능은 젊은이들에게 매우 필요한 조기 개입을 제공하며, 그들이 컴퓨터 사용과 오용에 관한 법을 이해하는 데 도움을 준다. 이는 잠재적인 범죄 활동의 위험 징후를 강조하고 사이버퍼스트, 직업으로서 사이버와 같은 이니셔티브를 통해 좋은 기회를 부각시켜 호기심이나 재능을 가진 사람에게 범죄 이외의 대안을 제시하고 범죄의 목적을 가진 사람들에게 이용당하는 것을 방지한다. 수잔은 끊임없이 모든 중고등학교에서 이용할 수 있는 학교 사이버 정보 프로그램을 개발했고 40개 이상의 초등학교, 수많은 중고등학교, 청소년 단체에 직접 참여했다. 이 젊은이들은 우리의 훌륭한 사이버 대사이자 미래의 수호자가 될 것이다.

목표 3:
우리의 국가 안보를 지키고 중대 범죄 예방 및 감지를 위해 사이버 공간에서 필요한 조치를 취한다.

186. 우리는 2025년까지 다음과 같은 성과를 달성할 것이다:

187. 영국의 사이버 능력을 키워 비사이버 위협을 억제하고 방해하는데 더 큰 영향력을 갖춘다. NCF(국가 사이버 군)의 규모를 상향하고 역량을 키워 NCF 로 하여금 정부통신본부 (GCHQ), 국방부 (MOD), 기밀 정보부 (SIS) 및 국방 과학 기술 연구소와 완벽하게 통합되고 법 집행 기관 및 기타 정부 조직과 긴밀히 협력하면서 이러한 핵심 역량에 대한 우리의 장기적인 비전을 실현하도록 할 것이다. 우리는 NCF를 통해 사이버 공간에서 책임감 있게 행동하고 모범을 보이는 적법하고 비례적인 공세적 사이버 작전을 수행할 것이다. 공격적인 사이버 작전을 통해 영국의 국방 및 외교 정책을 포함한 국가 안보와 중범죄 예방을 계속 지원할 것이다.

188. 우리는 또한 다른 위협에 대비해서 배치될 수 있는 인프라와 암호 화폐에 대한 법 집행 기술력을 스케일업하고 개발할 것이다.

189. 영국의 사이버 기능은 통합 운영 개념 2025에 따라 국방 작전 전반에 걸쳐 통합된다.[36] 이를 통해 적국에 대한 경쟁 우위를 유지하고 동맹 및 파트너와의 협력을 강화할 수 있습니다. 우리는 도메인 전체에 걸쳐 능력을 결합하고 국력의 다른 도구와 더 큰 통합을 제공하여 적국에 대한 군사적 우위를 강화하는 국방 다중 도메인 통합 변경 프로그램을 계속 진행할 것이다. 사이버는 고도의 기술을 갖춘 사이버 전문가, 국방 인력 전반에 걸친 전반적인 사이버 인식, 첨단의 탄력적인 사이버 능력에 의해 실현되는 국방 사업의 주류 부분이 될 것이다.

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

주요 법 집행 기관 사이버 범죄 수사

작전명 임페릴: 작전명 임페릴(Op Imperil)은 남동지역 조직 범죄팀이FBI와 공동으로 사이버 공격 피해자의 개인 정보 및 금융 정보를 판매하는 웹사이트를 수사한 사건이다. 이를 통해 다른 사람들이 개인 데이터를 구입하여 사기를 치고 더 나아가 컴퓨터를 악용한 공격을 가능하게 하였다. 상당한 조사를 통해 기술 인프라에 사용된 은행 계좌와 지불금의 확인으로 이어졌고 웹사이트 소유자가 파키스탄에 있다는 것을 확인했다. 이로 인해 FBI가 비밀리에 웹사이트를 장악하고 결과적으로 그 웹사이트를 무너뜨릴 수 있게 했다. 남동 지역 조직 범죄 팀은 범죄 자금 세탁을 위해 웹사이트 소유주를 대신하여 미국에 기반을 둔 은행 계좌를 개설한 것으로 밝혀진 주요 용의자를 체포했다. 영국인 용의자는 손상된 피해자 데이터 중 일부를 사용하여 은행 계좌를 다른 이름으로 개설하고, 손상된 은행 계좌를 사용하여 호화 휴가 비용을 지불하고, 노동연금부 허위 청구로 인해 9만 파운드가 넘는 국가에 손실을 입히는 중대한 사기를 저질렀다. 이 용의자는 9가지 혐의로 기소되었고 조기 유죄 인정으로 징역 4년을 선고 받았다. 판사는 조사단에 판사 표창을 수여했다. 출판 당시 몰수 및 평생범죄 수익법 적용이 진행 중이다.

작전명 니피곤: 이것은 불가리아 국적의 피의자가 영국에 4천만 파운드 이상의 손실을 입힌 것으로 추정되는 맞춤형 피싱 페이지를 만든 혐의를 받고 있는 것에 대한 런던 경찰청 수사였다. 이 피의자는 불가리아 국적인이 만든 피싱 페이지를 이용해 자신의 범죄에 사용하여 10년 형을 받은 유명한 사이버 범죄자에 대한 수사를 통해 밝혀졌다. 수사는 용의자와 관련된 중요한 이메일 주소가 확인됨에 따라 시작됐으며 용의자는 체포, 범죄인 인도, 그리고 포괄적인 공개를 통해 불가리아 당국과 협조 끝에 9년 6개월 구류형 유죄 판결을 받았던 사건이다.

작전명 리징: 2020년 COVID-19 대유행이 한창일 때 국가 범죄 수사처(NCA)는 국민 의료 기관(NHS)에 비트코인으로의 지불을 요구하며 테러 폭탄 위협을 한 용의자에 대한 수사를 주도했다. 독일 당국과 협력하여 NCA는 용의자의 신원을 확인하고 체포하여 독일 법정에서 성공적으로 유죄 판결을 받도록 하였다.

2020년 4월 12일, 독일에 거주하는 이탈리아 국적자는 TOR 네트워크를 통해 1,000만 파운드를 비트 코인으로 받지 않으면 NHS 병원을 폭격하겠다는 의사를 담은 이메일을 보냈다.

이 사건은 NCA에서 높은 최우선 순위 수사로 즉각 분류하고 사이버 범죄 전문 요원들이 가해자를 식별하고 잠재적인 공격을 예방하는 임무를 수행하였다.

가해자는 또한 의원들을 공격하고 런던의 흑인 시위대를 공격하고 폭탄 테러를 하겠다고 협박하는 이메일도 보냈다. 그의 이메일을 영어로 썼음에도 불구하고 NCA 조사관들은 전문적인 사이버 기술과 행동 및 언어 분석을 이용하여 범인이 독일어 원어민일 가능성이 높다고 추론했다.

독일 당국과 협력하여 NCA 관계자들은 이 이메일이 베를린에 있는 주소의 컴퓨터에서 발송된 것임을 확인했다. 국제적인 협력과 그의 신원과 위치를 숨기기 위한 상당한 노력에도 불구하고, 용의자는 독일 법 집행 기관의 감시를 받게 되었고, 2020년 6월 15일, 용의자는 강탈 미수 혐의로 체포되어 구금되었다. 그는 2021년 2월 26일 유죄를 선고받고 징역 3년을 선고받았다.

테러에 대응하기 위해 사이버 공간을 통한 조치 취하기

이슬람 극단주의자(Daesh) 대응 작전: 이슬람 극단 주의자에 대한 영국 국방부와 정부 통신 본부(GCHQ)의 노력은 인터넷과 현대 통신의 힘을 남용하는 사람들의 위협에 대응하기 위해 우리가 어떻게 적극적인 조치를 취해왔는지를 보여주는 예이다.

이슬람 극단주의자들은 테크놀로지 개발에 많은 시간과 에너지를 쏟았고, 과격화와 신입 요원 유치에 사용되는 미디어 콘텐츠를 제작했으며, 전 세계에 테러 공격을 유발했다. 최근 몇 년 동안 우리는 런던과 맨체스터의 공격을 포함하여 유럽 전역에서 이들의 이러한 접근법의 영향을 보아왔다. 이슬람 극단주의자들은 또한 그들의 전장 작전을 지휘하고 통제하기 위해 현대적인 통신 시스템을 사용했다. 이것은 그들이 규모와 속도에 따라 유연하게 활동할 수 있게 해주었고, 그들이 통제하고자 하는 지역민들에게 훨씬 더 큰 위험을 가할 수 있게 해주었고, 소위 칼리프 왕국에 대한 그들의 영향력을 극대화시켰다.

이슬람 극단주의자들이 수도로 자칭한 "모술 전투" 기간 동안, 우리는 연합군을 지원하는 군사 작전에 사이버 도구와 기술을 활용하였다. 이러한 작전의 결과는 광범위하여, 통신망 교란, 선전물 전파 방해, 내부 불신 유발, 작전의 일환으로 사용되는 장비·네트워크 부정 등 극단주의자들의 활동 효율을 저하하기에 매우 효과적인 방법을 초래하였다. 우리는 또한 사이버 기술을 사용하여 영국정부 정책 메세지를 홍보하고 예상치 못한 도움을 제공할 수 있는 사람들에게 정부의 활동을 강조할 수 있다. 이러한 작전을 통해 극단주의자들을 진압하기 위한 연합군의 노력에 큰 기여를 했고, 테러 공격을 조직하려는 그들의 계획을 방해했으며, 전장에서 연합 세력을 보호했다.

국가 사이버 군 일원 Andrew의 증언:

저는 항상 최신 테크놀로지의 매료되어 있었다. 정보기관에서 일하기 전에, 나는 경찰관으로서, 순찰 중인 순경에서 디지털 포렌식 전문가로 승진했습니다 - 증거를 찾기 위해 용의자의 전자기기를 살펴 보는 업무를 했죠. 그런 업무도 좋았지만 다른 기회가 있는지 보고 싶었어요.

학교를 졸업하고 대학을 가지 않았고 지금까지의 제 경력은 타고난 호기심에 이끌려 왔고, 국가 사이버 군에 입대하는 제 모든 동료들도 거의 비슷한 상황이었죠. 그들은 모두 다른 경력과 배경을 가지고 있습니다. 물론 가장 중요한 것은 우리들은 모두 깊은 기술적 전문성을 가지고 있는 공통점이 있지만, 전직 슈퍼마켓 지점장, 초등학교 교사, 소방관 경력을 가진 사람들이죠. 우리 모두의 공통점은 열린 마음, 배우려는 열망, 그리고 신 기술을 통해 새로이 떠오르는 국가 안보에 대한 위협과 기회 두 가지 모두에 대처하고자 하는 공동의 목표를 가지고 있죠.

과거에 경찰관으로서 나는 개인적으로 사람들을 돕는 것이 매우 자랑스럽게 생각해 왔고, 현재는 국가사이버군(National Cyber Force)의 독특한 팀의 일원으로서, 저는 전 세계적인 규모의 선의를 위해 싸우는 팀의 일원이 되었다.

우리의 목표 실현하기

190. 이 전략은 목표를 실현하고, 그에 대한 진행 상황을 모니터링하고 평가하고, 필요한 경우 방향을 조정할 수 있는 메커니즘을 갖추는 엄격한 접근법이 없다면 아무 의미가 없을 것이다. 이 장에서는 목표에 도달하기까지의 우리의 접근 방식을 설명하려고 한다.

범 정부적 역할과 책임

191. 국가 사이버 전략은 "통합 검토서"가 지향하는 바를 집합적으로 전달하는 하위 전략 중 하나가 될 것이다. 국가안전보장회의(NSC)는 이러한 전략들에 대한 장관들의 감독권을 행사하여, 이행을 감시하고, 영국 전략의 전반적인 균형과 방향을 검토할 것이다. 전략의 목표 대비 진행 상황은 "정부 계획 및 성과 프레임워크"와 "결과 성취 계획"을 통해서도 평가될 것이다.

192. 모든 장관들은 영국이 사이버 공간에서와 사이버 공간을 통해 자국의 이익을 보호하고 증진할 수 있도록 책임감 있고 민주적인 사이버 강국으로서의 입지를 굳건히 하게 하는데 역할을 담당하게 된다. 아래 목록에는 국가사이버전략의 5대 전략 축 중 하나 이상을 실행 또는 조정하거나 가장 중요한 사이버 역량과 결정을 감독하는 주도적 역할을 수행하는 장관들에 대한 구체적인 권한을 포함한다.

- 랭커스터 공국상은 예산처장의 조력을 받아 사이버 위협에 대한 효과적인 정부 대응과 사이버 강국으로서의 우리의 야심찬 목표를 달성하기 위해 부서 전반에 걸쳐 전반적인 리더십을 제공합니다. 여기에는 국가 사이버 전략의 개발 및 실행, 투자 지원 프로그램 및 사이버 복원력에 대한 정부 노력의 조정이 포함된다. 그들은 또한

사이버 보안과 영국의 중요한 국가 인프라의 복원력에 대한 전반적인 부문간 정책 및 조정 책임이 있다. 랭커스터 공국의 수상이 사이버 사건에 대한 장관급 국무 조정실 회의의 의장직을 당연직으로 행사한다.

- 내무부 장관은 국가 사이버 전략 전달과 국토 안보에 대한 책임에 부합하는 사이버 사건에 대한 대응에서 중요한 역할을 가진다. 내무부 장관은 외교 개발부 장관, 국방부 장관과 함께 우리의 적대국들을 탐지, 방해 및 저지하기 위한 정부의 작업을 주도하고 그 작업의 전반적인 조정을 제공한다. 그들은 또한 사이버 범죄에 대항할 구체적인 책임을 가진다.

- 외교 개발부 장관은 국가 통신 본부(GCHQ)와 국가 사이버 보안센터에 대한 법적 권한을 가진다. 장관은 사이버 분야에서 영국의 글로벌 리더십을 발전시키기 위한 정부의 작업을 이끌며 사이버 귀속 과정, 사이버 제재 체제 및 상위 범주의 사이버 사건에 대한 국제 협력에 대한 구체적인 책임을 가진다. 또한 내무부 장관, 국방부 장관과 함께 우리의 적대국들을 탐지, 교란, 저지하기 위한 정부의 업무를 주도한다.

- 국방부 장관은 외교 개발부 장관, 내무부 장관과 함께 우리의 적대국들을 탐지, 교란, 저지하기 위한 정부의 활동을 지휘한다.

- 외교 개발부 장관과 국방부 장관은 국방과 정보 간의 연합체로서 국가 사이버군에 대한 책임을 가진다.

- 디지털, 문화, 미디어 및 스포츠 장관은 디지털 정책과 관련된 더 넓은 경제의 조직들의 사이버 보안과 국가 사이버 전략의 관련 성장, 혁신 및 기술 측면을 주도한다. 영국의 사이버 생태계를 강화하고 사이버 파워에 필수적인 기술을 주도하기 위한 정부의 활동을 선도한다.

- 중요한 국가 기반 시설에 대한 모든 주요 정부 부서의 장관들은 해당 분야의 사이버 보안 및 탄력성 정책에 대한 책임을 가진다.

- 모든 장관들은 그들 부서의 사이버 보안에 대한 감독과 적절한 완화 조치를 제공해야 한다. 공공 또는 민간 부문(예: DLUHC, 지방 정부, DEFRA, 수자원 회사)의 요소를 감독하는 부서는 해당 부문과 관련된 사이버 정책과 활동을 책임진다.

193. 국가 정보, 안보, 복원력 담당 국가 안보 차장은 이 전략의 '선임 책임자'로서 부처 간 관련 고위관리의 지원을 받아 공식 차원에서 범 정부 목표 달성을 주도한다.

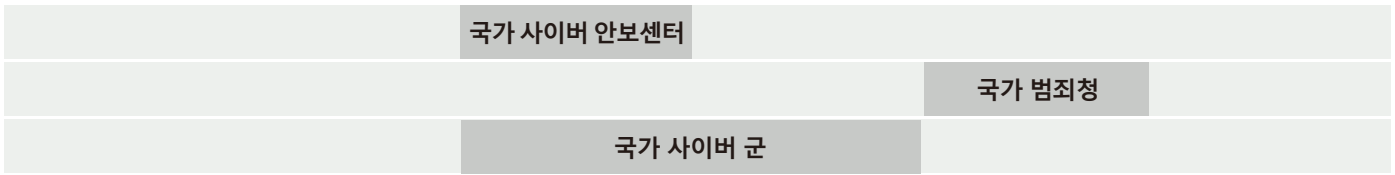
장관의 권한 범위

총리

전자부 장관	랭커스터 공국상*	외교부장관	국방부 장관	내무부 장관	장관 전체

전략축 조정 및 리더쉽 책임

전략의 운용 및 성취 지원



* 사이버 위협에 효과적으로 대응하고 사이버 전력으로서의 영국의 계획을 완성하기 위해 전 부처 간의 제반 리더쉽을 발휘한다.

우리의 사이버 전력에 대한 투자

194. 정부는 향후 3년간 사이버와 레거시 IT에 26억 파운드를 투자할 예정이다. 국가사이버군에 대한 상당한 투자는 이와는 별도의 예산이다. 상기 투자 예산에는 2016년 사이버 전략으로 구축된 능력에 대한 연간 지출과 함께 국가 사이버 보안 프로그램에 대한 추가 1억 1400만 파운드가 포함되어 있다. 이 예산은 부처간 예산 이동의 결과로 가능하게 되었다. 협력국을 지원하고 사이버 복원력을 구축하고 사이버 위협에 대응하기 위한 국제 프로그램이 분쟁안정안보기금(CSSF)을 통해 제공된다. 이는 R&D, 정보, 국방, 혁신, 인프라 및 기술 분야에서도 발표된 투자 증가와 함께 이루어지며, 이 모든 것이 영국의 사이버 파워에 기여하는 역할을 담당하게 될 것이다.[37]

성과의 평가

195. 이 전략에 대한 평가는 책임 고위 공직자와 국가안전보장회의(NSC)에 보고하는 지속적으로 진화하는 성과 체계로 이루어질 것이다. 이 체계(framework)은 국회와 국가 안보 공동체의 업무를 감독하는 다른 기관들과의 이루어지고 있는 협력 내용을 공지하는데 사용될 것이다. 국가사이버안보 전략 2016-2021의 접근 방식과 일관되게, 민감한 정보가 포함되어 있기 때문에 공개 문서는 아닐 것이지만 정부는 매년 진행상황 보고서를 발간할 것이다.

196. 이 성과 평가 틀을 가지고 다음을 수행할 것이다.

- 여러 활동이 전략서에 명시하고 있는 다양한 목표를 어떻게 이끌어 낼 수 있는지에 대한 명확한 경로를 제공한다.
- 전략의 달성 책임을 명확히 한다.
- 전략에서 설정한 목표를 향해 국가가 나아가고 있는 진행 상황에 대한 투명성을 제공한다.
- 전략에 맞춰 활동을 진행하기 위해 어떤 조율을 해야 하는지 방향을 제시한다.
- 전략적 야심찬 계획을 달성하는 데 효과적인 활동을 파악하여 향후 이러한 교훈을 적용할 수 있도록 한다.
- 중복을 줄이고 국가 사이버 전력 내의 강점과 약점을 파악하여 다섯 가지 주요 축에 걸쳐 활동에 대한 전반적 관점을 제공한다.
- 전략이 사회 전 분야에 사이버 지원을 제공하고 있는지 확인한다.

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

다음 단계

197. 이 전략은 사이버 및 기타 광범위한 관련 정책에 (별첨 A) 대한 책임이 있는 정부 관계자 뿐만 아니라 국가 사이버 노력에 대한 관심과 책임이 있는 사회 전체의 모든 개인과 조직을 위한 행동 지침으로 의도되어 만들었다. 이것은 또한 향후 5~10년 동안 우리의 목표와 우선순위가 관련성을 유지하도록 하기 위해 우리가 지속하고자 하는 대화의 시작이기도 하다. 우리는 이 전략의 발표를 영국 전역의 공공, 민간 및 제3 부문과의 추가적인 참여를 위한 플랫폼으로 사용할 것이며 ukcyberstrategy@cabinetoffice.gov.uk으로 이 전략에 대한 의견을 접수할 것이다. 우리는 매년 이 전략을 실행하기 위해 우리가 추진하고 있는 진행 상황에 대해 보고할 것이다.

별첨 A: 정부의 광의 어젠다의 일부로서의 사이버

국가 사이버 전략은 안보, 국방, 외교, 경제 어젠다 전체를 아우르는 정부의 우선 순위를 지원하고 확장하려는 의도로 만들어졌다. 그리하여 이 전략서가 교육과 기술 훈련 시스템, 디지털 기술 산업 정책, 연구 분야 및 기업의 성장에 대한 국가적 접근법을 통한 역량에 의존할 수 밖에 없을 것으로 생각된다. 이와 관련된 주요 전략과 계획으로는:

- 통합 검토서(integrated Review): 복원력을 개선하고, 국가적 위협에 대응하며, 중대 조직 범죄와 테러, 과학 기술을 통한 전략적 우위를 유지하며, 국제 질서를 세우고자 하는 국가적 노력을 포함하는 내용의 검토서

- 국가 데이터 전략: 생산성을 향상하고, 신생 기업과 일자리를 창출하며, 공공 서비스를 개선하고, 더 공평한 사회를 지원하며, 과학적 발견을 촉진하고, 영국을 혁신의 새로운 물결의 선도 국가로 자리매김하는데 데이터를 활용하는 역량에 박차를 가하려는 영국의 비전을 설명하는 내용

- 성장 계획: 추가적 지원과 인프라와 기술 훈련, 혁신 그리고 우리의 혁신 주도형 경제를 위한 우리의 야심찬 계획인 혁신 전력에의 투자를 통해 영국이 더욱 성장하도록 도와 줄 수 있는 계획

- 디지털 규제에 대한 계획: 번영을 촉진하고 디지털 기술을 사용함에 있어서 신뢰를 구축하는 방향으로 디지털 기술을 규제하고자 하는 영국의 친 혁신적 접근법을 설명하는 계획

- 국가 AI 전략: 영국이 다가오는 변혁의 시기에 잘 대비하도록 준비하려는 목표를 가진 전략. 이는 AI 생태계의 장기적 요구에 투자를 하고, AI 가 가능하게 하는 경제로의 전환을 지원하고, 영국이 AI 기술에 대한 권리를 국내적 그리고 국제적으로 조정할 수 있도록 함으로써 대비시켜야 한다.

- 곧 발표할 국가 회복력 전략: 사이버 공간에서 영국이 테크놀로지성 위협으로 부터 회복력을 유지할 것인가에 집중한 전략

- 곧 발표할 디지털 전략: 디지털 전환에 대한 새로운 관심을 촉진하고, 성장을 촉발하며, 보다 포용적이고 경쟁력 있으며 미래 혁신 디지털 경제를 형성해 가려는 정부의 야심찬 계획에 대한 명확한 비젼을 설명하는 전략. 이 전략은 문화미디어 스포츠 부의 10개 테크 우선 순위를 바탕으로 준비하는 것으로 디지털 분야에서의 정부의 야심찬 계획을 더욱 구체화하는 것을 의미한다.

- 네트 제로 전략: 영국의 번영하는 혁신 주도형 경제를 저탄소 경제로 가능하게 하려는 전략·범죄 퇴치 계획: 법 정의 시스템에서의 자신감을 회복하고 범죄를 줄이고 피해자를 줄이는 더 안전한 영국에 대한 공동 비전을 성취하기 위한 방법을 설명하는 계획[38]

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

국가 사이버 전략을 직접 보완하는 2개의 문서가 추가 발간될 예정이다. 이 문서는 국가 사이버 전략의 개별 부분이 어떻게 성취될 것인지를 설명하는 문서이다.

- **곧 발표할 정부 사이버 보안 전략:** 국가 사이버 전력의 조력을 받아 정부와 공공 분야의 보안을 강화하고자 하는 구체적 계획을 설명하는 전략.

- **곧 발표할 2021년 인센티브와 규제 리뷰:** 광의 경제 안에서 사이버 보안의 개선점을 찾도록 인센티브를 주고자 한 정부의 노력이 얼마나 효과적이었는지를 분석하고 회복력의 축을 기업과 기관에서 어떻게 실행하게 하는 것이 좋을 지를 설명해 주는 검토서.

별첨 B: 네트워크 및 정보 시스템 (NIS) 규제 - 국가 전략

개요

NIS 국가 전략

1. 국가 사이버 전략은 영국의 국가 전략으로서, 영국 2018 NIS 규정의 2항에 목적을 가지고 만들어진 전략이다.

2. 여기에서는 추가적 정보를 아래와 같이 제공한다.

- 영국내 NIS의 실행을 책임지는 주요 기관의 역할과 책임 범위
- 관련 주요 기관 목록

영국 NIS 규정

3. 2016년 유럽 의회에서는 EU 내의 NIS 보안을 향상할 목적으로 시행령에 합의를 했고 이 시행령에 영국 정부도 합의했다.

4. 2018년 4월 20일에 영국 정부는 의회에서 2018 NIS 규정을 개정하여 발표하였다. 이 규정은 2018년 5월 10일 시행되었다.

5. 이 NIS 규정으로 영국내 새로운 규정 체제를 마련한 것으로, 필수 서비스의 지정 운영자과 관련 디지털 서비스 제공자들이 자신들의 네트워크와 정보 시스템을 안전하게 보호하기 위한 기술적, 자체적 조치를 마련하도록 요구하는 규정이다.

6. 이 규정은 에너지, 교통, 상수도, 보건 및 디지털 인프라 등 네크워크와 정보 시스템에 의존도 높은 부문이며 우리 경제와 사회에 필수 불가결한 부문에 적용한다.

7. 주요 디지털 서비스 제공자(검색 엔진, 클라우드 컴퓨팅 서비스, 온라인 마켓 등)도 이 규정에 규제를 받게 된다.

8. NIS 규정은:

- 국가 전략을 포함한 시행을 지원하기 위한 국가적 틀을 만들고,
- 부문별로 경쟁력 있는 기관을 규제 담당 기관으로 지정하며,
- 국가 사이버 보안 센터(NCSC)를 단독 담당 기관(SPOC) 및 컴퓨터 보안 사건 대응 팀으로 지정한다.

9. 이와 관련한 진전 상황은 매 2-5년 마다 실행 검토를 통해 평가한다.

주요 역할과 책임 범위

국가 프레임워크

10. 국무조정실에서는 NIS 국가 전략으로 구성된 국가 사이버 전략을 담당한다. 국무조정실은 또한 중대 국가 인프라의 보안과 복원력을 개선하는 총괄적 책임을 가진다.

11. 디지털, 문화, 미디어, 스포츠부(DCMS)에서는 NIS 규정의 총괄적 시행에 대한 권한을 가지며, 이는 NCSC와 관련 기관 간의 조율 권한을 포함한다. DCMS 부는 전 영국에 걸쳐 NIS 시행을 지원하기 위해 관련 기관에 지침을 내려 준다.

전담 사고 보고 담당 기관 (SPOC)

12. NIS 관련 국제적 파트너(EU)와의 모든 협력의 국가 담당 기관으로서, 정보와 조치를 요청하고 받는 조정 역할을 하고 연차 사건 통계를 제공하는 역할을 맞게 된다. 국가 사이버 보안 센터(NCSC)가 영국의 전담 담당 기관(SPOC) 이다.

컴퓨터 보안 사고 대응팀 (CSIRT)

13. 국가 사이버 보안 센터(NCSC)가 영국의 CSIRT 이다. 이 곳에서는 국가 수준에서 사이버 보안 사건을 모니터하는 책임을 가지고 실시간 위협 분석과 국가 사이버 공격에 대항하여 방어하고, 기술적 지원과 피해를 최소화 하도록 주요 사이버 사건에 대한 대응을 제공하는 기관이다.

14. NCSC에서는 결과 기반 사이버 평가 프레임워크를 갖추고 국가 기술 기관으로서 사이버 보안 문제에 광범위한 가이드를 제공한다.

책임 기관:

15. 이들은 NIS 규정에서 요구하는 사항에 OES(필수 서비스 운영자)와 RDSP(관련 디지털 서비스 제공자)들이 따르고 있는지를 평가하고 지정함으로써 규정이 잘 지켜 지는지에 대한 권한을 가진다. NIS 규정 1조와 3항에 목록과 권한이 기술되어 있다.

필수 서비스 운영자(OES)와 관련 디지털 서비스 제공자(RDSP)

16. 각 분야의 위임 권한을 가졌거나, NIS 규정의 8.3 항에 의거 관련 권한을 위임받은 필수 서비스 운영자(OES)나 관련 디지털 서비스 제공자(RDSP)은 반드시 NIS 규정을 준수해야 한다.

17. 반드시 준수해야 하는 사항에는:

- 네트워크과 정보 시스템 보안에 발생하는 위험 요소를 관리하기 위한 적절한 기술적 그리고 기관 차원의 조치를 취해야 한다.
- 네트워크과 정보 시스템에 영향을 주는 사건의 충격을 최소화하고 방지하는 적절한 조치를 취해야 한다.
- 당 기관에서 제공하는 서비스에 상당한 영향을 주는 사건에 대해서는 모두 관련 책임 기관에 고지해야 한다.
- NIS 규정에 의거 감사 요건을 맞추어야 한다.
- 정보, 시행 그리고 벌금 고지에 따라야 한다.
- 관련 디지털 서비스 제공자는 또한 ICO에 등록을 요한다.

기타 관련 기관

18. 영국 정부는 위임 정부와 기타 관련 기관과 NIS 규정의 시행에 대해 긴밀하게 협력한다.

19. CPNI (국가 인프라 보호 센터)에서는 관련 물리적 인적 보안과 관련한 조언을 제공한다.

NIS 시행 관련 주요 기관 목록

국가 기관	
영국 NIS 규정	디지털, 문화, 미디어, 스포츠부
영국 국가 사이버 전략	국무조정실
영국 단일 담당부처	국가 사이버 보안 센터
영국 컴퓨터 사건 대응 팀	국가 사이버 보안 센터

책임 기관					
부문	**하위 부문**	**영국**	**웨일스**	**스코틀랜드**	**북아일랜드**
에너지	전기	공동: 기업, 산업, 에너지 전략부/가스 전기청			재무부
	석유	기업, 에너지 산업 전략부			재무부
	가스	공동: 기업, 산업, 에너지 전략부/가스 전기청[39]			재무부
교통	항공	공동: 교통부/시민 항공청			
	열차	교통부			재무부
	해상	교통부			
	도로	교통부		스코틀랜드 장관	재무부
보건	보건 제도	보건 사회부	웨일스 장관	스코틀랜드 장관	재무부
상수도	상수도	환경, 식품, 농업부	웨일스 장관	스코틀랜드를 위한 음용 수질 조절기	재무부
디지털 인프라	디지털 인프라	통신부			

[39] 예외적으로 기업, 에너지, 산업 전략부가 유일한 책임 기관이 되기도 한다. 이에 대한 보다 자세한 사항은 2018 네트워크 및 정보 시스템 규정의 1조와 2조를 참고한다.

별첨 C: 용어 사전

Action Fraud – 시민과 기관에서 잉글랜드, 웨일즈 및 북아일랜드에서 사기, 또는 사이버 범죄를 경험한 경우 사기 및 사이버 범죄에 대해 신고해야 하는 신고 센터. 스코틀랜드는 스코틀랜드 경찰에 신고해야 한다.

Active Cyber Defence (ACD) – 기관이 취약점을 찾아 교정하고, 사건을 관리하거나 사이버 공격으로 인한 혼란을 막을 수 있도록 도와주는 기관. 주로 공공 부문을 위해 설계되어 있지만, 비공공 분야 및 시민들도 사용 가능하도록 만들어 졌다.

인공 지능 (Artificial Intelligence) – 자율적으로 적응하고 운용되어 "스스로 생각하도록" 코딩 되어진 컴퓨터 시스템 기술. AI는 의료 진단, 의약품 발견, 예지 보전 등과 같은 매우 복잡한 업무를 수행하는데 점점 더 이용되고 있다.

인증 – 신원 확인, 사용자, 프로세스 혹은 기기의 속성을 확인하는 프로세스

자율 시스템 – 특정한 개체 혹은 도메인의 관리하에 절차가 이루어지게 하기 위한 IP 네트워크 집합

블록체인 기술 – 데이터를 저장하는 특별한 방법. 블록체인은 (네트워크상의 다수의 컴퓨터로 처리되는) 분산 원장의 일례로서, 첨부 전용, 변조 방지 저장 기술임.

COBR – Cabinet Office Briefing Rooms (국무회의 브리핑 룸). 영국 중앙정부의 비상사태 대응은 COBR을 통해 뒷받침된다; 주로 웨스트민스터에 위치하여, 가장 중요한 대응이 시행, 모니터링 및 조정되며, 정부의 대응과 지역 대응에 대한 당국 조언의 핵심을 제공한다.

주무 관청 – 네트워크 및 정보 시스템 (NIS) 규정 2018에 기술되어 있는 담당 관청. NIS에 의하여 cover되는 여러 분야를 다수의 주무 관청이 책임지고 있다.

연결 장소 – 정보통신 기술과 IoT 기기를 통합하여 데이터를 수집 및 분석하여 기 구축된 환경에 새로운 서비스를 제공하고, 시민들의 삶의 질을 향상시키는 커뮤니티.

국가 중요 인프라 – 손실 혹은 손상이 야기될 수 있는 인프라의 중요 요소 (즉, 자산, 설비, 시스템, 네트워크 또는 프로세스와 이를 운용하고 촉진하는 필수 인력)

a. 중대한 경제적 또는 사회적 영향을 고려한 – 무결성이 훼손될 경우 상당한 인명 또는 사상자 손실을 초래할 수 있는 서비스 포함하여 – 필수 서비스의 가용성, 무결성 또는 제공에 미치는 중대한 해악.

b. 국가의 안보, 국방 혹은 기타 국가 기능에 미치는 중대한 영향

암호키 (CK) – 가장 강력한 적의 공격으로부터 영국 정부, 군사 및 국가 안보 공동체가 의존하는 중요한 정보와 서비스를 보호하기 위해 영국이 사용하는 암호술을 표현하는 데 사용되어 지는 용어.

암호화폐 – 비트코인과 같은 디지털 통화 및 결제 시스템.

암호술 – 암호와 암호를 분석하고 해독하는 학문 또는 연구; 암호 분석.

CAF (Cyber Assessment Framework) – 필수 기능에 대한 사이버 위험이 담당 조직에 의해 관리되고 있는 정도를 평가하기 위한 체계적이고 포괄적인 접근 방식을 제공한다.

사이버 공격 – 컴퓨터 시스템, 디지털 의존적 기업 및 네트워크에 해를 야기하는 의도적이고 악용.

사이버 범죄 – 사이버 의존적 범죄 (ICT 장비를 통하여 저지르는, 그 장비가 도구이자 범죄의 대상이 되는); 또는 사이버 지원 범죄 (금융 사기처럼 ICT 장비 없이도 저질러질 수 있지만, ICT 장비의 사용에 의해 그 범위나 규모가 현저하게 확대될 수 있는 범죄).

사이버 생태계 – 상호 연결된 인프라, 인력, 프로세스, 데이터, 정보 및 통신 기술의 총체. 그리고 이러한 상호작용에 영향을 미치는 환경 및 조건의 총체.

사이버 사고 (Cyber Incident) – 컴퓨터, 인터넷 연결 장치, 네트워크 – 또는 이러한 시스템에서 전송, 저장 처리되는 데이터에 – 실제로 또는 잠재적으로 위협을 가하는 사건의 발생으로, 결과를 완화하기 위한 대응 조치가 필요한 사고.

사이버 복원력 – 사이버 사고를 이겨내고, 피해가 발생한 경우 그 것을 복구하는 시스템, 조직 및 시민의 전반적인 능력.

사이버 위험 – 주어진 사이버 위협이 정보 시스템의 취약성을 악용하여 해를 끼칠 수 있는 가능성.

사이버 보안 – 인터넷 연결 시스템 (하드웨어, 소프트웨어 및 관련 인프라 포함), 데이터 및 이러한 시스템이 제공하는 서비스를 무단 액세스를 통하여 손상 또는 오용으로부터 보호하는 것. 여기에는 시스템 운영자에 의해 보안 절차를 따르지 않거나 조작되어 발생한 우발적, 혹은 고의적인, 피해를 포함한다.

사이버 보안 지식단 (CyBOK) – 모든 사이버 보안 분야에 걸쳐 지식 체계를 최초로 제공하는 고유한 기관으로서, 사이버 보안이 매우 광범위한 분야에 걸쳐 적용된다는 것을 보여준다.

사이버 위협 – 정보 시스템 및 인터넷 연결 장치 (하드웨어, 소프트웨어 및 관련 인프라 포함), 데이터 및 서비스에 대해, 주로 사이버 수단을 통해 보안을 손상시키거나 피해를 입힐 수 있는 모든 것.

데이터 위반 – 정보에 접근하거나 정보를 볼 권한이 없는 당사자에게 네트워크에서 정보를 무단으로 이동 또는 공개하는 행위.

도메인 – 도메인 이름은 인터넷상의 조직 또는 그 외의 개체의 위치를 나타내며, IP (인터넷 프로토콜) 주소와 일치한다.

이양 정부 또는 이양 행정부 – 스코틀랜드, 웨일스 및 북아일랜드의 분리된 입법부와 행정부로서, 이러한 분야에 대한 법률을 제정할 수 있는 권한을 갖고 많은 국내 정책 문제를 담당하고 있음.

Digital Twin (현존하는 대상의 디지털 버전) – 기 구축된, 사회 또는 자연 환경에 있는 자산, 프로세스, 시스템 또는 기관을 가상 복제하거나 표현한 것으로, 물리적 자산과 시민이 어떻게 행동하는지 통찰력을 제공하여 조직이 의사 결정을 개선하고 프로세스를 최적화하는 데 도움을 준다. 현실 세계의 변화가 디지털 버전에 반영되고, 디지털 버전에서의 변화가 현실 세계에서 자동으로 복제될 수도 있다.

Five Eyes – Five Eyes는 미국, 영국, 캐나다, 호주 및 뉴질랜드 간의 정보 동맹으로, 위협으로부터 자국민을 최대한 안전하게 보호할 수 있도록 정보 공유를 돕고 있다.

GCHQ – Government Communications Headquarters(정부 커뮤니케이션 본부); 정부의 신호 정보 활동 및 사이버 국가 기술 기관 (NTA)을 위한 센터.

GFCE – Global Forum on Cyber Expertise. 사이버 전문가의 글로벌 포룸

GCCC (Government Cyber Coordination Center) – GSG, CDDO 및 NCSC 간의 공동 벤처 제안으로 정부 전체의 사이버 보안 노력을 운영적인 측면에서 보다 효과적으로 조정하고, 사이버 보안 데이터 및 위협 정보가 정부 기관 전체에 어떻게 사용되는지 혁신하고, 하나가 되어 방어하는 정부의 능력을 진정으로 향상시킨다.

Horizon Scanning – 잠재적인 위협, 리스크, 새로운 문제 및 기회를 식별하기 위한 체계적인 정보 검사로, 정책 결정 과정에 있어서의 (부당한) 이용과 완화에 대한 조정, 더 좋은 대비를 제공한다.

ICANN – 인터넷 주소 관리 기구 (Internet Corporation for Assigned Names and Numbers). 웹사이트 이름과 IP 주소를 조정한다.

사고 관리 – 시스템이나 네트워크에 손상을 입히거나 손상을 입힐 수 있는 사이버 사건의 실제 또는 잠재적 발생을 조사하고 해결하기 위한 활동의 관리 및 조정.

사고 대응 – 사고의 단기적이고 직접적인 영향을 다루고 단기적인 복구를 지원하는 활동.

산업 제어 시스템 (ICS) – 제조, 제품 취급, 생산 및 유통과 같은 산업 프로세스를 제어하거나 인프라 자산을 제어하는 데 사용되는 정보 시스템.

통합 검토 – '경쟁 시대의 글로벌 브리튼, 안보, 국방, 개발 및 외교 정책에 대한 통합 검토'는 향후 10년간 영국의 역할에 대한 정부의 비전과 2025년까지 정부가 취할 조치에 대해 설명한다.

무결성 – 정보 보안에서 무결성은 정보가 우발적으로 또는 의도적으로 변경되지 않고 정확하고 완전함을 의미한다.

인터넷 – 글로벌 컴퓨터 네트워크로, 표준화된 통신 프로토콜을 사용하여 상호 연결된 네트워크로 구성된 다양한 정보 및 통신 기능을 제공한다.

사물 인터넷 (IoT) – 인터넷을 통해 통신하고 데이터를 교환하는 전자 장치, 소프트웨어 및 센서가 내장된 장치, 차량, 건물 및 기타 항목의 전체.

레거시 IT – 레거시 IT는 공급업체 지원 범위를 벗어나거나, 확장 지원 및/또는 맞춤형 지원 계약을 맺고 있는 시스템과 해당 구성 요소의 소프트웨어 및 하드웨어를 의미한다.

관리형 서비스 공급자 – 고객에게 일련의 정의된 서비스를 제공하고 해당 서비스의 실행, 유지 및 보안을 책임지는 제3자.

자가 전력 (microgeneration) – 가정, 소기업 및 지역사회에 의한 소규모 에너지 생성.

나토 – 북대서양 방위 기구

NCA – 국립 범죄국

국립 사이버 보안 센터 (NCSC, National Cyber Security Centre) – 사이버 위협에 대한 영국의 기술 당국으로서 사이버 사고에 대한 손해를 최소화하기 위한 통합된 국가 대응을 제공하고, 미래를 위한 복구 및 학습에 도움을 준다.

NIS (Network and Information Systems) 규정 2018 – 필수 서비스 및 디지털 서비스 제공을 위해 네트워크 및 정보 시스템의 보안 수준(사이버 및 물리적 복원력 모두)을 높이기 위한 법적 조치를 제공하는 영국 규제.

OECD – 경제협력개발기구. 정부간 경제기구

공격적인 사이버 – 실제적, 가상 또는 인지적 효과를 주기 위해 시스템 또는 네트워크의 데이터를 추가, 삭제 또는 조작하는 것. 공격적 사이버 운영은 종종 기술적 취약점을 이용하고, 소유자와 운영자가 의도하지 않거나 묵인하지 않는 방식으로 시스템이나 네트워크를 사용하며, 속임수나 사칭에 의존하기도 있다.

운영 기술 (OT) – 하드웨어 및 소프트웨어를 통합하여, 특히 에너지, 제조, 수자원, 운송과 같은 산업 분야의 물리적 프로세스를 모니터링, 제어 및 자동화하는 기술.

필수 서비스 운영자 – NIS 규정 2018의 기준에 규정된 유틸리티, 의료, 운송 및 디지털 인프라 부문과 같이 정보 네트워크에 크게 의존하는 필수 부문 내의 조직.

디지털 규제 계획 – 성장과 혁신을 추진하기 위해 디지털 기술을 관리하는 정부의 전반적인 접근 방식을 제시한다.

양자 기술 – 양자 기술은 양자 물리학의 원리에 의존한다. 중첩과 얽힘과 같은 '양자 효과'로 알려진 것에 대한 이해와 통제는 감지, 데이터 전송 및 암호화, 타이밍 및 컴퓨팅과 같은 우리의 경제와 사회를 뒷받침할 새로운 발전의 물결을 이끌 것이다.

랜섬웨어 – 몸값이 지불될 때까지 파일, 컴퓨터 또는 장치에 대한 사용자의 액세스를 거부하는 악성 소프트웨어.

Secure by Design – 처음부터 안전하게 설계된 소프트웨어, 하드웨어 및 시스템.

취약성 – 공격자에 의해 악용될 가능성이 있는 소프트웨어 프로그램의 버그.

취약성 보고 서비스 – 조직이 공격자에 의해 악용되기 전에 보안 결함을 알릴 수 있는 메커니즘.