HM Government

国家サイバー戦略 2022

英国全体のサイバーの未来を開拓するために

国家サイバー戦略 2022

英国全体のサイバーの未来を開拓するために

内容目次

追加内容

前書き

英国はオープンで民主的な社会です。コラボレーションとイノベーションの実績をもとに、世界に広く目を向けるグローバル国家として成功を収めてきました。このことは、健康医療の国際緊急事態への対応や、気候変動対策におけるネットゼロ目標の推進に示される通りです。しかしこの英国のアプローチが最も強みを発揮するのは、サイバー分野をおいて他にありません。

我々は、国全体の均等なレベルアップと団結を目指す中で、サイバーが国民と経済にもたらす幅広い利益を認識するとともに、様々なパートナーと協力しつつ英国の国家的価値を反映するサイバー空間の実現に取り組んでいます。あるいはまた、サイバー能力をフル活用して、地球規模の出来事に影響力を行使しようとしています。英国は、テクノロジーを通じて再編されつつある世界において国益を保護し増進するひとつの手段として、サイバーをとらえています。

ここにご紹介する最新の国家サイバー戦略は、英国が日々目まぐるしく進展するデジタル世界において自信と能力とレジリエンス（回復力）を維持しながら、サイバー空間における国益の保護・増進のために適応、革新、投資を継続していくための計画です。

2016年に発表した先駆的な「国家サイバーセキュリティ戦略」を引き継ぐものとして、本新戦略は、サイバー攻撃に対する英国のレジリエンスをさらに強化していくことを目指します。私はこの課題に主導的責任をもつ大臣として、2つの中心目的を明確にしています。その一つは、サイバーに不可欠な技術分野で英国の能力を強化することであり、もう一つは、個々のサプライヤーや、英国の価値観とは相容れない体制下で開発された技術への依存を減らしていくということです。

英国の科学技術はこの変革の推進役となるでしょう。サイバーが国の経済的・戦略的資産であり続けることが保証され、英国の技術の信頼性が高まるとともに、様々なサイバー敵対者が最近まで国家的専有物だった能力を手に入れ実行し始めた攻撃を撃退する能力も高まるはずです。

英国政府は研究開発に220億ポンドを費やし、テクノロジーを国家安全保障計画の中心に置くと約束しています。デジタル技術がもつ変革への潜在力は周知の通りですが、例えば5Gが示すように、そこには破壊的な潜在力もあります。AI（人工知能）とデータ政策に関する英国の計画は、デジタル技術分野の最先端国家になるためのものです。また、サイバー戦略に基づく様々な措置によって、サプライヤーやパートナーのセキュリティとレジリエンスに対しても自信を強めることができます。

昨年の国家サイバー部隊（NCF）の創設は、攻撃力の高いサイバー能力の向上にとって大きな一歩となりました。とはいえ基本的なサイバーセキュリティも、引き続き、英国と英国市民を攻撃者から守る対応強化の取り組みの中心を占めています。さらに、公共部門のレジリエンスを固め、自治体がそれぞれのシステムや市民の個人情報をランサムウェアやその他のサイバー攻撃から守れるよう支援することも、重点のひとつです。

社会として、サイバーはあらゆる人の利益のためにあります。英国政府は本戦略を通じて、国民と企業、そしてパートナー諸国を守るためにさらなる努力を重ねていきます。そして、サイバー空間を、信頼性とレジリエンスに優れ、人々とビジネスが繁栄する場にするというビジョンを実現していきます。

ランカスター公領大臣兼内閣府担当大臣
スティーブ・バークレー下院議員

イントロダクション

デジタル時代の機会と課題

1. 世界は技術の飛躍的進歩とコストの低下を背景に、かつてないほど緊密につながり、多大な機会とイノベーション、そして進歩を推進している。この傾向は新型コロナウイルス感染症（COVID-19）の大流行で加速された。とはいえ、現在はまだ、長期的な構造転換の初期段階に過ぎないと考えられる。サイバー空間のグローバルな拡大により、生活、仕事、コミュニケーションのしかたは変化しており、金融、エネルギー、食料流通、ヘルスケア、輸送等の様々な分野に欠かせない重要システムの姿も変貌しつつある。端的に言えば、サイバー空間は今や我々の将来の安全保障と繁栄にとって必要不可欠となっている。そしてそこには、英国のような技術先進国が新しいやり方で国家目標を追求することのできる絶好の機会が存在する。

2. このような変化の規模とスピードは多大で、これまでの社会規範や法律、民主主義の諸制度がそれに追いつかない場合も多く、しかも前例のない複雑さ、不安定、リスクの要因となっている。昨年は、病院や石油パイプライン、学校、企業がサイバー攻撃を受け、ランサムウェアによって機能停止を余儀なくされたところもあった。また、様々な活動家や、ジャーナリスト、政治家を標的とした商業スパイウェアも使用された。サイバー空間には国境超越的な性質があり、国際協力なしに問題に対処することは不可能である。それと同時に、全システム的な競争や、対立する利益、価値、グローバルな未来像が衝突する場としても、サイバー空間の重要性は高まっている。

英国のビジョン：国家目標の基盤となるサイバーパワー

3. このような背景から、サイバーパワーは国力増強の手段および戦略的優位の源泉として、これまで以上に重要性を増している。**サイバーパワーとは、国益の保護と増進を、サイバー空間の内部およびサイバー空間を通じて実現する能力である。**これからは、デジタル時代の機会と課題をうまく乗り切れる国こそが、安全でレジリエンス（回復力）が強く、繁栄する国となる。英国は世界有数のデジタル先進国であり、政府は国内外で野心的なテクノロジー計画を推進している。そのためサイバー空間の様々な問題には敏感であるが、同時に、国民および人類共通の利益のための機会を活用できるユニークな主導的立場にあると言える。

4. 今後10年間、インターネットと、それを支えるデジタル技術およびインフラが、英国の利益、そして英国の同盟国や敵対国の利益にとっても、これまで以上に重要性を増すだろう。競争激化の時代における英国の新しい役割を固めていく上で、サイバーパワーを強化すれば、産業界と他の国々をリードして将来の技術変化に先手を打ち、脅威を緩和し、敵対国や競合国に対して戦略的優位を獲得することが可能になる。そしてそれにより英国は、人が暮らし、事業に従事し、投資を行うのに最も安全で魅力的なデジタル経済を実現できるだろう。

5. 英国のビジョンは、**2030年も引き続き責任ある民主的サイバー大国としての地位を保ち、サイバー空間の内部およびサイバー空間を通じて国益を保護・増進しつつ以下のような国家目標を追求していくこと**である。

- 進化する脅威とリスクに備え、国民を犯罪や詐欺、外国国家の脅威から守るためにサイバー能力を活用する、より安全でよりレジリエントな国になること。
- 国全体と多様性あふれる国民全体に機会が均等に行き渡り、イノベーション力の高い繁栄するデジタル経済を実現すること。
- 環境に優しい健康的な社会に向けて、革新的な技術を安全に活用する科学技術大国になること。
- グローバルな舞台で強い影響力をもつ価値あるパートナーとなり、サイバー空間での行動の自由を維持しつつ、オープンで安定した国際秩序の将来像を形成していくこと。

6. 過去10年間、英国はサイバー大国として確立し、最先端のサイバーセキュリティとオペレーション能力、および、先進的なサイバーセキュリティセクターを築いてきた。本戦略は、「国家サイバーセキュリティ戦略 2016-2021」のもとで実現した進捗、および、政府の「安全保障・防衛・開発・外交政策に関する統合レビュー」が示す3つの重要な結論に基づいて策定された。第一に、デジタル時代において、英国のサイバーパワーは国家目標の実現にとってこれまで以上に重要な手段となる。第二に、サイバーパワーを維持していくには、サイバーのあらゆる目的と能力を考慮に入れた、より包括的で統合的な戦略が必要である。第三に、全社会的アプローチが必要である。英国のサイバーパワーにとって、企業の役員室や学校の教室で起こることは、技術専門家や政府高官の行動と同程度に重要である。英国が成功するには、様々なパートナーシップを築いて協力することが欠かせない。


CHELTENHAM
Science
Festival
18.2 Cyber Skills a
@CyNam

英国の戦略を支える5つの柱

7. 政府の「統合レビュー」は本戦略の5つの優先行動を定めており、ここではそれを戦略的枠組みの5つの柱として活用する。それぞれの柱は、**英国が取るべき具体的行動と、2025年までに達成したい成果を整理し、手引きとして示している**。

- **第1の柱：英国のサイバーエコシステムを強化する。**人材とスキルに投資し、政府・学術界・産業間のパートナーシップを緊密にする。
- **第2の柱：レジリエントで豊かなデジタル国家を構築する。**サイバーリスクを削減することによって企業はデジタル技術の経済利益を最大化し、国民はオンラインの安全性と個人データの保護に関する信頼性を享受できる。
- **第3の柱：サイバーパワーに死活的重要性をもつ技術を先導する。**産業の能力を増強し、将来のテクノロジーを確保する枠組みを構築する。
- **第4の柱：より安全で、豊かで、開かれた国際秩序のために、英国のグローバルなリーダーシップと影響力を増進する。**政府および産業界のパートナーと協力し、英国のサイバーパワーの基盤となる専門知識を共有する。
- **第5の柱：サイバー空間の内部およびサイバー空間を通じた英国の安全保障の強化のために敵対者を検知し、攪乱し、抑止する。**英国が持つあらゆる手段を、より統合的、創造的、日常的に活用する。

8. 本文書の第1部では、英国を取り巻く戦略的な状況と、英国の戦略の目標、および、今後10年間にとるべき戦略的アプローチについて説明する。第2部では、2025年の目標達成のために取るべき具体的行動を、5つの柱に沿って整理する。

ビジョン

英国は2030年も責任ある民主的なサイバー大国であり続け、国家目標を追求しながら、サイバー空間の内部およびサイバー空間を通じて国益を保護し増進していく。

それぞれの柱と目的

第1の柱

英国のサイバーエコシステムを強化する

1. サイバーへの全社会的アプローチを支援するのに必要な構造、パートナーシップ、ネットワークを強化する。
2. あらゆるレベルで国家のサイバースキルを強化・拡充する。ここには、世界トップレベルの多様なサイバー専門職へと将来世代の人材を育成することも含まれる。
3. 持続可能で革新的、かつ国際競争力を持つサイバーおよび情報セキュリティセクターの成長を促進しつつ、政府や経済全体のニーズに応える高品質の製品・サービスを提供する。

第2の柱

レジリエントで豊かなデジタル国家を構築する

1. サイバーリスクへの理解を深め、サイバーセキュリティおよびとレジリエンスに関する効果的な行動を促進する。
2. サイバー攻撃をより効果的に防止しこれに抵抗するために、英国の組織内のサイバーリスク管理を改善し、国民の保護を強化する。
3. サイバー攻撃に備え、対応し、そこから回復するために、国と組織レベルでレジリエンスを強化する。

第3の柱

サイバーパワーに死活的重要性をもつ技術を先導する

1. サイバーパワーにとって死活的重要性をもつ科学技術の発展を予測、評価し、それに基づいて行動する能力を高める。
2. サイバー空間に必要不可欠な技術の安全保障に関して、主権国家および他国の同盟国としての優位を育成し維持する。
2a. 堅牢でレジリエントな国家的暗号キー(Crypt-Key)事業を継続していく。この事業は、英国政府の顧客、パートナー諸国、同盟国のニーズを満たすとともに、最強の敵対者からの脅威をも含めて最も重大なリスクを適切に軽減する実績をあげている。
3. 次世代のコネクテッドテクノロジーおよびインフラを確保しつつ、グローバル市場への依存で生じるサイバーセキュリティリスクを軽減し、英国のユーザーに信頼性の高い多様な供給へのアクセスを確保する。
4. マルチステークホルダーコミュニティと協力して、グローバルなデジタル技術標準の開発に寄与する。特に、民主主義的価値の擁護、サイバーセキュリティの確保、英国の科学技術を通じた戦略的優位の推進に関わる分野を優先する。

第4の柱

英国のグローバルなリーダーシップと影響力を増進する

1. パートナー諸国のサイバーセキュリティとレジリエンスを強化し、敵対者を混乱させ抑止するための集団的活動を増強する。
2. 自由でオープンで平和で安全なサイバー空間を推進するために、グローバルガバナンスを形成する。
3. 英国のサイバー能力および専門知識を活用して輸出し、戦略的優位を高め、より広範な外交政策と繁栄のための利益を促進する。

第5の柱

敵対者を検知し、攪乱し、抑止する

1. 英国とその利益および国民を守るために、国家、犯罪者、その他悪意のあるサイバー行為者と活動を検知し、調査し、情報共有する。
2. 英国とその利益および国民を狙った、国家、犯罪者、その他悪意のあるサイバー行為者と活動を抑止し、攪乱する。
3. 国家安全保障と重大犯罪の防止・検知を支援するため、サイバー空間の内部およびサイバー空間を通じた対策を実行する。

支援する国家目標

- セキュリティとレジリエンス
- 科学技術大国
- 経済的繁栄
- 国際秩序の形成

第1部：
戦略


CyberFirst Girls Competition 2020
1 The Tiffin Girls' School 805
2 The Castle School 760
3 Herschel Grammar School 665
4 The Cathedral School 660
5 King Edward's School 635
6 Stretford Grammar School 580
7 Greenwood Academy 520
8 Loughborough High School 455

戦略的背景

競争時代における グローバルブリテン

9. 2021年3月に発表された「安全保障・防衛・開発・外交政策に関する統合レビュー」は、今後10年間の世界における英国の役割について、政府のビジョンと、2025年までに取るべき行動を説明したものである。世界的な競争の激化に備えていくには、科学技術のイノベーションを取り入れて国の繁栄と戦略的優位を強めていかなければならないことを、英国は認識している。国家サイバー戦略はこのようなアプローチに基づいており、その発表は、「統合レビュー」の戦略目標である「科学技術を通じた戦略的優位の維持」のもとで実行するコミットメントの一つである。

サイバーをめぐる状況

10. サイバー空間に関わる政策課題は、単なる技術的性格のものにとどまらない。サイバー空間は人間が作り出した環境であり、基本的に人間の行動により形成されている。人間の行動は良くも悪くも増幅され、その影響は通常、現実の世界でも感得される。サイバー空間を所有し運営するのは、民間企業、政府、非営利団体、個々の一般市民であるほか、犯罪者もこれに含まれる。つまり、このような状況に戦略的に対応するには、地政学的戦略と国家安全保障、刑事司法と民間規制、経済政策と産業政策を関連付けるとともに、多種多様な文化的・社会的文脈と価値体系がオンラインで相互作用することに関する深い理解が必要である。

11. サイバー空間は国境も超越する。現在、テクノロジー分野のサプライチェーンと重要依存関係はますますグローバル化している。一方、サイバー犯罪者と国家の後援を受ける行為者が世界中で活動している。また、強力なテクノロジー企業は製品を輸出してその基準設定を行い、サイバー空間とインターネットを支配するルールと規範は国際的な協議を通じて決定されている。サイバー空間は、技術や人々の利用方法の変化に伴って絶えず進化するため、機敏なアプローチが必要である。

サイバースペースの各層

サイバー空間とは？

多くの人にとって、サイバー空間とは、コミュニケーションや仕事、日常の様々な用事をこなすためにインターネットを利用する際に体験する仮想世界のことである。しかし専門的用語としてのサイバー空間は、インターネット、通信ネットワーク、コンピュータシステム、インターネット接続機器等を含む、相互依存的な情報技術ネットワークを意味する。一方、軍隊にとって、あるいはサイバー空間の脅威への対抗策の検討においては、サイバー空間は陸、海、空、宇宙と並ぶ作戦領域の一つである。

サイバー空間はどのように経験されるか？サイバー空間は、定義上、「共有された」空間であり、その規模と複雑さのためにすべての人の経験はそれぞれ異なる。市民は、オンラインで銀行口座をチェックしたり、自宅で映画をストリーミング再生する時にサイバー空間にアクセスする。企業は、社員を必要なリソースへとつなげる際に（例えば情報へのアクセスや、製造工程の管理など）、サイバー空間を利用する。政府は、国民に公共サービスを提供するためにオンラインのポータルを利用する。サイバーの専門家は、ユーザーにとってすべてが適切に機能するよう、技術や標準、プロトコルといったサイバー空間の「内部事情」を扱う。これらすべての集団が様々な方法と目的でサイバー空間を利用しており、誰もが皆、ますますその利用を増やしている。

オンライン体験	• 電子メールアカウント • ゲーミングプロフィール • ソーシャルメディアのアカウント • 銀行口座へのログイン • コンタクトレス交通カードID • フィットネストラッカープロフィール
ソフトウェア、システム、データ	• 企業ITシステム • 各種データベース（英国歳入関税局の徴税記録等） • 産業用制御システム • Windows/OS • アプリ（例えば、WhatsApp、Facebook、TikTok） • プログラミング言語、Python, C++
物理的デバイスとコミュニケーション	• ルーター、ハブ • サーバー • WiFi、イーサネット • 無線アンテナ • スマート冷蔵庫 • コンタクトレス交通カード読み取り機 • 電話、パソコン、その他のパーソナルデバイス

サイバースペースは3つの層から構成される。

仮想層

サイバー空間のうち、最も多くの人が体験する部分である。共有された仮想空間において仮想アイデンティティを通じて表現される人および組織が、これを構成する。仮想表現の例としては、電子メールアドレスや、ユーザーID、ソーシャルメディアアカウント、通称名が挙げられる。1人または1つの組織がオンラインでは複数のアイデンティティを持つことが可能である。また逆に、複数の人や組織がただ一つの共有IDを作成することもできる。

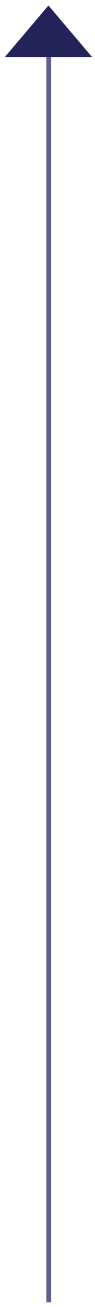
論理層

サイバー空間のうち、コードやデータで構成される部分である。

例えば、オペレーティングシステム、プロトコル、アプリケーション、その他ソフトウェア等がこれにあたる。論理層は物理層なしには機能せず、情報は有線ネットワークや電磁波スペクトルを介して伝えられる。論理層は物理層とともに、仮想アイデンティティがコミュニケーションをとり行動することを可能にする。

物理層

サイバー空間の物理層には、個人が自宅で使うルーター、ワイヤ、ハブ等、データ送信のためのハードウェアから、大手ハイテク企業が運営する大規模で複雑な通信システムまで、様々なものが含まれる。また物理的インフラだけでなく、WiFiや無線等のデータ送信のための電磁波もここに含まれる。



サイバーパワー

12. 英国の戦略の中心にあるのはサイバーパワーの概念である。これは「国家がサイバー空間の内部およびサイバー空間を通じて国益を保護し増進する能力」と定義される。ここでは、本戦略の5つの柱に沿って、サイバーパワーがもつ広範な5つの次元を次のように特定する。

- サイバーパワーの基盤となる人、知識、スキル、構造、パートナーシップ。これらは他のすべての構成要素を下支えしつつ国家的アプローチへと統合する。
- サイバーセキュリティとレジリエンスを通じて英国の資産を保護する能力。その目的は、サイバー空間が国民と経済にもたらす恩恵をフルに実現することにある。
- 重要サイバーテクノロジーの進化に対して深い関与を続け、社会的利益になる新たな進歩を実地展開できる技術的および産業的な能力。
- サイバー空間のルールと規範を英国の価値観と利益に沿って形成し、国際安全保障および安定を促進することのできるグローバルな影響力、協力関係、倫理基準。
- 国家安全保障、経済的繁栄、犯罪防止に役立つ行動を、サイバー空間の内部およびサイバー空間を通じて実行できる能力。ここには、実社会で効果を発揮し、戦略的優位を獲得するためのサイバーオペレーション、悪質なサイバー犯罪者を裁き、その活動を妨害するための法執行やサイバー制裁の適用などが含まれる。

13. サイバーパワーは、従来型のパワーとは一線を画する。そこには、ハードな能力とソフトな影響力のシームレスな融合が含まれる。サイバーパワーは分散的であり、政府がこれを獲得して行使するには、様々なパートナーとの協力が不可欠である。また、技術が急速に変化し、最先端能力も新たな進歩によってすぐに陳腐化するため、サイバーパワーは一気に獲得されたり失われたりする。

14. 本戦略はこの点を考慮に入れており、政府は全社会的な取り組みの一環として、様々なパートナーと可能な限り協力していく必要がある。問題は発生の上流部分で対処して根本原因を解決する必要があり、将来のトレンドを予測し、長期的対応を実施し、紛争が多発する地政学的環境においては、後手に回ることなくそれを積極的に形成していくことが求められる。

今日のサイバー大国としての英国

15. 英国はすでに先進的サイバー大国として発展を遂げている。[1] 過去10年間、政府は、英国のサイバーセキュリティを強化し、サイバーリスクへの国民の意識を高め、サイバーセキュリティセクターを育成し、敵対的行為者からの脅威に対抗するサイバー空間を通じた幅広い能力を開発するために、国家的取り組みを持続的に主導してきた。それは大きく前進し、英国は確固たる地位を築いたが、依然として本戦略の5つの柱に関わる重大な課題の数々に直面している。

[1] 国際電気通信連合の「グローバル・サイバー・セキュリティ指数」で第2位、ハーバード・ベルファー・センターの「サイバーパワー指数」で第3位、国際戦略研究所の「サイバーパワー能力評価」で第2層にランクされている。

英国のサイバーエコシステムとテクノロジーリーダーシップ

16. 英国のサイバーパワー構築へのアプローチは、英国政府と、北アイルランド、スコットランド、ウェールズの各自治政府がパートナーシップを築いて互いの経験を活かしつつ、国全体のサイバースキル基盤と商業能力を開発していくための協調的取り組みを含んでいる。英国のサイバーセキュリティセクターは急成長しており、昨年は1400社を超える企業が89億ポンドの収益を上げ、4万6700人の熟練雇用を支えるとともに、海外から多額の投資を誘致している。同セクターはサイバーパワーにとって死活的に重要であり、英国の安全保障と国際的影響力および経済成長の支えとなるものである。英国はサイバーセキュリティ研究のグローバルリーダーとして評判を固めており、19の卓越研究センターと4つの研究機関が喫緊のサイバーセキュリティ課題に取り組んでいる。

17. サイバーセキュリティセクターの労働人口は過去4年間に約50パーセント増加し、スキルへの需要が供給を上回るケースも多い。英国政府は、サイバーセキュリティスキルに関する課題の本質をよりよく理解すべく、産業界、専門家団体、学生、雇用者、既存のサイバーセキュリティ専門家、および学術界と幅広い協力関係を築いている。また、サイバーセキュリティ分野でのキャリアを目指す若い世代に向けて、関心を高めるためのイニシアチブを多種多様に実施している。2019年から2020年にかけては、学習プログラムとして「サイバーファースト」と「サイバーディスカバリー」を実施し、およそ57,000人の若者が参加した。また、低年齢層向けのコースも実施し、例えばオンラインの競技イベント「サイバーファースト・ガールズ」には11,900人の女子生徒が参加し、最後まで残ったトップチームが国内18の会場で同時に競い合った。サイバーファースト奨学金プログラムも、意欲的で優秀な大学生の関心を引いている。昨年は学生750名がこの制度を活用し、56名の卒業生は全員がサイバーセキュリティ分野のフルタイムの職に従事している。

18. しかしこのような政府の介入にもかかわらず、広範なスキル不足は引き続き大きな課題である。経済全体の企業132万社のうち約半数が、サイバーセキュリティの基本的技術スキルに不足があると報告している。[2] また、英国のサイバーセキュリティセクターは急成長しているものの、そのほとんどが新興企業であり、大規模な国内ベンダーの構築は国際的な企業統合が進む中、依然として困難な課題である。5Gの経験が示したように、英国と英国の同盟国は、広範なテクノロジー産業の一部重要分野で主導的地位を逃している。サイバーパワーに必要不可欠な技術で主導的役割を確立できれば、そのような技術の設計と配備の方法に影響力を行使でき、自国の安全保障と経済的優位を守り、サイバー能力の飛躍的向上の機会をより迅速に活用することが可能になる。

英国のサイバーレジリエンス

19. 過去10年間、政府は英国のサイバーレジリエンスの強化を目指して様々な介入策を実施してきた。これを可能にしたのは多額の持続的投資であり、その対象は、国家サイバーセキュリティセンター（NCSC）や、法執行機関、政府全体のセキュリティおよび政策専門家といった英国の中核的サイバー能力に加え、国内外の様々なパートナーシップの拡充にも及ぶ。

---

[2] デジタル省、Cyber security skills in the UK labour market 2021（「2021年の英国労働市場におけるサイバーセキュリティスキル」）(2021年)

20. 最も革新的かつ画期的な取り組みは、積極的サイバー防衛（ACD）プログラムの開発・拡大展開を始めとする大規模な対策の実施である。ACDプログラムは昨年、NHSのブランドを悪用したフィッシング詐欺442件や、公式アプリストア以外でホストされダウンロード可能な違法のNHSアプリ80件を含む、230万件の悪質な組織的活動を削除した。[3] 英国はまた、接続可能な消費者向け製品について、設計段階でセキュリティを組み込んだ「セキュアバイデザイン」にする取り組みを世界に先駆けて進めてきた。2018年には英国実施規則を策定して他国の範となり、インターネット接続される消費者向け機器に関する、世界的に適用可能な初の業界標準に有益な情報を提供した。[4] [5]

21. 新たな規制はサイバーセキュリティに好影響を及ぼし、2018年の英国一般データ保護規則の導入に影響を受けて改善措置を取ったとする組織は82パーセントに上った。[6] また今日、77パーセントの企業がサイバーセキュリティを優先課題と捉えており、これは2016年比で12パーセントの増加である。[7] 2018年のネットワーク・情報システム規制（以下「NIS規制」）の導入後、指定組織はネットワークや情報システムのセキュリティを確保する対策を講じ、必要不可欠なサービスや重要デジタルサービスへのサイバーリスクの軽減を実現した。[8] NIS規制の実施を含む医療分野での改善措置は、英国の4つのネーションにおける協力関係の好例となった。

22. 英国政府は経済全体の諸組織に対して、総合的なサイバーセキュリティ関連のアドバイスおよびガイダンスを提供してきた。また、新型コロナウイルス感染症（COVID-19）のパンデミック時には重要セクター向けに個別の支援を行った。一般市民に対しては「サイバーアウェア」キャンペーンを実施し、ネット上で自分自身を守るためにできることをアドバイスしている。また実際にサイバー攻撃が発生した場合には、世界トップクラスの事故対応能力を駆使し、特に深刻なケースには直接支援を提供するとともに、報告されるすべての事故に対応できるよう現地の法執行機関の専門家に資金を投じている。

23. 政府は専門の法執行機関サイバーユニットを英国全土に、またこれと並んで、サイバーPROTECTネットワーク、経済犯罪被害者ケアユニット、さらに各地域にサイバーレジリエンスセンターを設置している。これらの取り組みにより、市民や中小企業・組織は、適切なスキルと地元の知識を持つ人物が近隣にいて容易に連絡ができ、サイバーレジリエンス向上のためのサポートやガイダンスを得ることができるようになっている。

---

[3] 国家サイバーセキュリティセンター（NCSC）、NCSC Annual Review 2021（「NCSC年次レビュー2021」）(2021年)

[4] デジタル省、Code of Practice for Consumer IoT Security（「消費者向けIoTセキュリティの実施規則」）(2018年)

[5] デジタル省、ETSI industry standard based on the Code of Practice（「実施規則に基づくETSI業界基準」）(2019年)

[6] デジタル省/RSM, The impact of GDPR on cyber security outcomes（「GDPRがサイバーセキュリティの結果に及ぼす影響」）(2020年); 2018年に英国法に導入された一般データ保護規則（GDPR）は、現在、英国GDPRに置き換わっている。

[7] デジタル省、 Cyber Security Breaches Survey 2021（「サイバーセキュリティ侵害調査 2021」）(2021年)

[8] デジタル省、Post-Implementation Review of the Network and Information Systems Regulations 2018（「ネットワーク及び情報システム規則2018の実施後レビュー」）(2020年)

24. しかし、国レベルのレジリエンスには数々の問題点のあることが、ますます明らかとなっている。というのも、政府、企業、個人に影響を及ぼすサイバー犯罪や違反行為が、サイバーで可能となる詐欺等の犯罪も合わせて、レベルアップし続けているからである。[9] [10] 特に懸念されるのは、ITシステムのレガシー化や、サプライチェーンの脆弱性、サイバーセキュリティの専門家の不足である。企業の10社に4社（39%）とチャリティ団体の4分の1（26%）が、過去1年間にサイバーセキュリティの侵害や攻撃を受けたと報告しており、多くの組織（特に中小企業）は、自衛し事故対応する能力が不足している。[11] 産業界が述べているように、多くの企業が現実のサイバーリスクを理解しておらず、サイバーセキュリティに投資する商業的インセンティブも明確でない上、違反行為や攻撃を報告する動機がほとんど存在しない場合も多い。

英国の国際的なリーダーシップと影響力

25. 国際的に見て、英国のサイバー関連専門知識はパートナー諸国から高く評価されており、悪意のあるサイバー活動と対決する国際的能力と決意の増進に役立ってきた。これに寄与したのは、英国の攻撃型サイバー能力の責任ある活用である。それは一部敵対者の無差別的活動とは対照的に、英国法および国際法と英国が公言する立場に則っている。

26. 英国は英連邦議長国を務めた期間中に、サイバー空間における安全、繁栄、価値観への共通のコミットメントである「英連邦サイバー宣言」を作成し、実施を主導した。また国家犯罪対策庁（NCA）の国際ネットワークは、長年の共同作戦対応で培った協力関係に基づいて、海外のサイバー法執行機関とのパートナーシップを強化している。さらに、サイバーおよび技術セキュリティ担当者の海外ネットワークを5大陸に拡大し、世界100カ国で能力開発を実施して、レジリエンスを構築し、英国の影響力を高め、英国の価値観を推進している。

27. サイバーセキュリティ・アンバサダープログラムは、長期的な関係を築き、英国企業が重要な国際契約を獲得するのに役立っている。また、デジタルアクセスプログラム等の国際開発援助は、アフリカ、アジア、ラテンアメリカのパートナー諸国と協力しつつ、各国政府、産業界、ユーザーのサイバーセキュリティ能力の強化に向けて技術的アドバイスを提供している。例えば、サービスが不足しているコミュニティでサイバー衛生スキルの訓練を行い、ネット上のリスクや課題から最も脆弱な人々でも自衛できるようにしている。

28. しかし英国は、様々なアプローチの国際的競争状況に直面している。中国やロシアのような全システム的競合国が、安全保障上の対策として、サイバー空間に対する国家主権の拡大を主張し続けているからである。インターネットの自由度は世界的に低下しており、開かれた社会の間で知識や財の交換を支援する共有空間としてインターネットをとらえるビジョンも、脅かされている。

---

[9] コンピュータ不正利用禁止法違反として定義される

[10] 国家統計局、Crime in England and Wales: year ending June 2021（「イングランドとウェールズの犯罪：2021年6月までの1年間」）(2021年)

[11] デジタル省、Cyber Security Breaches Survey 2021（「サイバーセキュリティ侵害調査2021」）(2021年)

英国に向けられるサイバー脅威への対策と、敵対者の抑止

29. 近年、英国がサイバー空間の内部およびサイバー空間を通じて直面する脅威は、強度、複雑さ、深刻さを増している。スパイ行為、商業的利益、妨害活動、偽情報を目的に英国を狙うサイバー攻撃者は、国家主体や、犯罪集団（国家の指示や暗黙の承認のもとに行動することもある）、活動家等、多種多様に拡大している。このような攻撃は多額の経済的損失や、知的財産の盗難、心理的苦痛、サービスや資産の混乱、そして、重要国家インフラ、民主主義の制度、メディアに対する様々なリスクを引き起こす。また、投資家や消費者の信頼感にもダメージを与え、既存の格差や害悪を増幅させることもある。新型コロナのパンデミック期間中は、影のパンデミックとも呼ばれる女性に対する暴力が、オンライン攻撃によってさらに深刻化した。ランサムウェアの攻撃は引き続き巧妙化し、被害が拡大している。パンデミック期間中の敵対行為者によるサイバー脅威は、全体的なレベルとしては安定的だったが、彼らはこれを好機と捉えて作戦を変え、ワクチンや医療研究を盗んだり、すでに危機的状況に陥っている他国に危害を加えたりしている。また、リモートワークやオンライン取引等でデジタル技術への依存度が高まっていることも、リスクを高める結果となっている。さらに、デジタルデバイドがオンラインサービスへのアクセスに関して格差を生んでいる。デジタルリテラシーやサイバーセキュリティ対策は誰もが安全にネットを利用できるようにするためのものであるが、それらの理解が限られている人が、ネットでのいじめや危害にさらされる事態となっている。[12]

30. 政府はこのような脅威の増大に対応するため、様々な対策を取っている。まず、情報（インテリジェンス）能力への大規模投資により、脅威への理解が深まり、より効果的な秘密の対抗作戦の実施が可能になった。また、国家犯罪対策庁（NCA）と、イングランド、ウェールズ、北アイルランド、スコットランド全体の地域的組織犯罪ユニットおよび地方警察内のサイバー専門チームが主導して、サイバー犯罪への統合的な法執行対応を展開している。これにより、サイバー犯罪者やその他の敵対者への作戦および捜査上の優位が強化された。政府はまた、増加の一途をたどるデジタルアイデンティティ・ソリューションのセキュリティ強化のため、英国デジタルアイデンティティ及び属性信頼フレームワークを策定した。[13] これはアイデンティティデータを悪用した犯罪への対処に役立つであろう。さらに、NCAの「サイバーチョイス」プログラムは、人々がより多くの情報に基づいて選択できるよう支援するとともに、犯罪に巻き込まれることなくポジティブかつ合法的にサイバースキルを利用するよう促している。

31. 英国政府は攻撃型サイバー能力に多額の投資を行ってきた。国家攻撃型サイバープログラム計画を手始めに、最近では国家サイバー部隊（NCF）も創設した。NCFは、政府通信本部（GCHQ）、国防省（MOD）、秘密情報部（SIS、通称MI6）、国防科学技術研究所から人員を集め、一つの統合的な司令のもとに結集した初の組織である。英国の安全を守り、国益を内外で保護・増進することを目的として、サイバー空間の内部およびサイバー空間を通じて活動している。

[12] 国家サイバーセキュリティセンター、CyberAware（サイバーアウェア）
[13] デジタル省、UK digital identity and attributes trust framework（「英国のデジタルアイデンティティ及び属性信頼フレームワーク」）(2021年)

32. 英国は同盟国とも連携して、国家による後援を受けたサイバー攻撃のコストを高めるべく、攻撃のアトリビューションや（最近のSolarWinds社やMicrosoft Exchange社の侵害事件で実施の通り）、責任者に結果を課すことを試みた。このように英国の自律的なサイバー制裁体制の整備によって、破壊的威力をもつツールがまた一つ新たに加わり、実際にWannaCryやNotPetyaといった攻撃への対応に使用された。しかしながらこのような前進にもかかわらず、英国のサイバー抑止のアプローチはなお、攻撃者のリスク計算を根本的に変えるには至っていない。以下に挙げるのは、最近発生した重大なサイバー攻撃の例である。

最近のサイバー攻撃の事例

2021年、英国は世界のパートナー諸国と協力して、共通の脅威を検知し破壊するための活動を継続した。そのような脅威の中でも特に一貫性の高いものはロシアと中国から発信されていた。ロシアからの脅威については、国家による直接的なサイバーセキュリティの脅威のほか、欧米を標的にランサムウェア攻撃を仕掛ける組織犯罪集団の多くがロシアに拠点を置いていることが明らかになった。中国は依然としてサイバー空間におけるきわめて巧妙な行為者であり、国外に影響力を行使する野心を強めるとともに、英国の商業機密への関心も高いことが証明されている。おそらく今後10年間の中国の行動が、英国のサイバーセキュリティの将来にとって唯一最大の促進要因となるだろう。イランと北朝鮮もまた、ロシアや中国ほどで巧妙なものではないものの、デジタル侵入を続けており、窃盗や破壊工作等を通じて自らの目的を達成しようとしている。

公共サービスを狙ったランサムウェアによるサイバー犯罪

2021年の英国にとって最も重大なサイバー脅威となったのは、ランサムウェアである。NCSCは、ランサムウェアの攻撃が成功した場合に必要不可欠なサービスや重要国家インフラに及ぶとみられる影響に基づいて、ランサムウェアを外国国家によるスパイ行為と同等の有害性を持ちうると評価した。[14]

2020年10月には、ロンドン自治区の一つであるハックニー・カウンシルがランサムウェアによるサイバー攻撃を受け、何カ月にもわたる混乱が生じ、修復に数百万ポンドを費やした。新型コロナ・パンデミックの影響に対応していた重要な時期に、同カウンシルは重要データを利用できなくなり、カウンシル税や各種福祉手当を始めとする多くのサービスに支障をきたした。同様の攻撃は他の地方自治体や、教育分野の様々な組織にも及んだ。

[14] 国家サイバーセキュリティセンター、Mitigating malware and ransomware attacks（「マルウェアとランサムウェアの攻撃を軽減するために」）(2021年)

2021年5月、アイルランド保健サービスエグゼクティブ（HSE）がランサムウェアの攻撃を受け、アイルランドの医療ITネットワークと病院が10日以上にわたって混乱し、患者とその家族が実際的被害を被った。また患者のデータの一部が盗まれ、ネット上で公開された。アイルランドで医療・社会福祉サービスを提供するHSEは、同日、事故を封じ込めるために全国と地域のネットワークを停止した。悪質なサイバー行為がアイルランド保健省（DoH）のネットワークでも検知されたが、捜査過程で各種ツールを導入した結果、ランサムウェア実行の企てを検知し阻止することがでた。このサイバー攻撃は北アイルランドにも影響を与え、HSEが保有し南北アイルランドで共有されている患者サービスのデータへのアクセスに支障が出た。

重要なのは、いずれのケースでも、データの身代金は支払われなかったことである。**法執行機関が身代金要求の支払いを奨励、保証、容認することはない。身代金を支払った場合、**

- **その後にデータやコンピュータにアクセスできる保証はない。**
- **利用しているコンピュータは感染したままである。**
- **犯罪集団に資金を供給することになる。**
- **今後ターゲットにされる可能性がさらに高まる。**

NCSCは、マルウェアやランサムウェアの攻撃から組織を守るためのガイダンスを公開し、攻撃に備える方法や、組織がすでに感染している場合に取るべき手順を説明している。

外国国家による戦略的脆弱性とサプライチェーンの悪用

ソフトウェア企業SolarWindsの情報漏洩と、Microsoft Exchangeサーバーへの攻撃は、サプライチェーン攻撃の脅威を浮き彫りにした。この2件の巧妙な攻撃は、経済、政府、国家安全保障機関のサプライチェーンにあるセキュリティの低い要素（例えばマネージドサービスプロバイダーや商用ソフトウェアプラットフォーム等）を標的としたもので、NCSCがこれまでに観測した中で特に深刻なサイバー侵入だった。

2020年12月初め、米国のサイバーセキュリティ企業のFireEyeが、同社と世界の他の多くの組織が使用している製品に対して、攻撃者が悪意のある改造を加えることが可能だったことを発見した。攻撃者はこの改造を通じて、影響を受けた製品のインストールに管理者レベルのコマンドを送信でき、接続されたシステムを標的にしてさらに攻撃を仕掛けた可能性があった。最初のサプライチェーン攻撃は、**SolarWinds**社が開発したITネットワーク監視ツールのソフトウェア「Orion」を通じて発生した。行為者は悪意のあるコードを、同ソフトウェアのアップデートファイルに2020年3月まで遡って埋め込むことが可能だった。2021年4月にNCSCは、米国のセキュリティ機関とともに、ロシア対外情報庁（SVR）がこの攻撃の背後にいたことを初めて明らかにした。これは最近の最も深刻なサイバー侵入の一つだった。[15] SolarWinds社が確認したところによれば、米政府機関を含む世界18,000の組織が被害を受けた。この事件は、NATO加盟国や欧州各国政府のITネットワークへのアクセスを試みるという、SVRが以前より行っている広範なサイバー侵入パターンの一部だった。

---

[15] 外務省、Russia: UK and US expose global campaign of malign activity by Russian intelligence services（「ロシア：英国と米国、ロシア情報機関によるグローバルな悪意ある活動を暴露」）(2021年)

2021年3月2日、マイクロソフト社は**Microsoft Exchange**サーバーの多くが巧妙な攻撃を受けたと発表した。同サーバーは世界中の組織が電子メール、スケジュール、コラボレーションの管理のために使用している。同社の評価では、最初の侵入が始まったのは2021年1月であり、中国国家が関与していた。これを受けて同社は、影響を受けたサーバー向けに複数のセキュリティアップデートをリリースした。英国は2021年7月にパートナー諸国とともに、中国国家を後ろ盾とする行為者が、世界25万以上のサーバーに及んだ攻撃に責任を負うと確認した。[16] この攻撃は、個人を特定できる情報や知的財産の取得を含む、大規模なスパイ活動を可能にするものと考えられた。Microsoft Exchangeに攻撃を加えることで、行為者は、被害組織のITネットワークにさらに深く入り込む足がかりを得たのである。攻撃発生時に政府は被害組織に対して迅速にアドバイスと推奨措置を提供し、マイクロソフト社は92パーセントの顧客が3月末までに脆弱性に対するパッチを適用したと発表した。

[16] 外務省、UK and allies hold Chinese state responsible for a pervasive pattern of hacking（「英国と同盟国、蔓延するハッキングパターンについて中国国家の責任を追及」）(2021年)

変化への原動力

33. 今後10年間、**データおよびデジタル接続は生活のほぼすべての側面に急速に拡大し続けるだろう。**インターネットへのアクセスと利用が、データとデータ利用を可能にするインフラに支えられて世界全体で大きく拡大し、新たな市場の創出や、利便性、選択肢、効率性の増進を実現している。しかし、それは同時に、各国が相互接続されたデジタルシステムへの依存を強め、悪意のある活動の機会が増え、現実世界に多大な影響を及ぼすことを意味する。重要テクノロジーと非重要テクノロジーのセクター横断的な融合が続いている現在、これらのリスクは経済の新たな分野に広がり、しかもデータとサービスのクラウド化（多くの場合は英国外への移動を意味する）によってリスクがさらに高まる事態となっている。

34. 現在、電気通信やエネルギー等の規制対象セクターの安定企業と、マイクロ発電や電気自動車充電設備、あるいはコネクテッドプレイス機能の提供事業といった、大部分規制されていない新興企業との間で相互作用がますます拡大している。今後、重要インフラはいっそう普及、拡散していくだろうが、それにより、必要不可欠な重要機能・サービスのセキュリティに対する規制のあり方も根本的変化を余儀なくされる。このような多様化は広く国家安全保障にも影響を及ぼし、法執行やサイバーセキュリティのための情報でもアクセスはより難しくなる。こうした環境の変化はさらに、従来型の重要国家インフラ以外の製品やサービスにも広く影響を及ぼすであろう。

35. このように**ますます複雑化する状況**において、国家や企業や社会は現実的なリスクと自衛の方法を理解することがいっそう困難となるだろう。マネージドサービスを提供するサードパーティへの依存が高まっているが、サードパーティは多数の顧客のITシステムに特権的にアクセスできる場合が多く、新たなリスクとして対応が求められている。デバイスやネットワークはますますインターネット接続が標準化し、家庭、自動車、建造環境、産業インフラにもサイバー空間が拡大していくだろう。また、センサー、ウェアラブル、医療機器、バイオメトリクスによって、オフラインとオンラインの活動の境界も曖昧化していく。サイバーリスクが蔓延し、個人情報や機密情報の生成が増えるとともに、システムが侵害された場合の潜在的影響も大きくなるだろう。

36. このような情勢のもと、**サイバー空間における脅威は引き続き進化し、多様化していく**だろう。ハイエンドのサイバー能力が商品化され、より広範囲の国家や犯罪集団へと拡散していくためである。サイバー空間で英国を狙う能力と意図を持つ行為者は増加し、様々な国家が、代理行為者の利用を含む幅広い手段で破壊的活動を行うようになるだろう。パンデミックの影響でハイブリッド型ワークへの移行が加速し、国際的な往来も制限されたことで、デジタルサービスへの依存が高まり、組織的犯罪集団がサイバー犯罪を犯す動機となった。その傾向を示すサインはすでに表れており、最新犯罪調査の概算では2019年から2021年にかけてサイバー犯罪が大幅に増加した。[17] この問題は英国に限られず、サイバー空間に依存するすべての人と社会に相互的な脆弱性をもたらしている。

[17] 国家統計局、Crime in England and Wales: year ending June 2021（「イングランドとウェールズの犯罪：2021年6月までの1年間」）(2021年)

37. サイバー空間の争奪戦は今後さらに激化する。国家と非国家主体がサイバー空間の内部およびサイバー空間を通じて戦略的優位を追求するためである。サイバー作戦は、閾値未満の武力紛争や紛争前段階状況での戦力投射にとって次第に重要になるだろう。将来の紛争ではサイバー能力の利用も増加するはずである。英国が効果的に行動するには、防衛能力におけるサイバーレジリエンスのレベルアップが必要である。サイバー作戦は、脅威を撃退して広範な防衛活動を可能にするために、他の部隊要素と統合されなければならない。宇宙もまた、国家宇宙戦略が示したように、今後は次第に一つの活動領域となり、数々の新たなリスク分野を生むだろう。しかし同時に、英国がサイバー能力を活用して新たな方法で優位性を獲得する機会にもなるはずだ。[18]

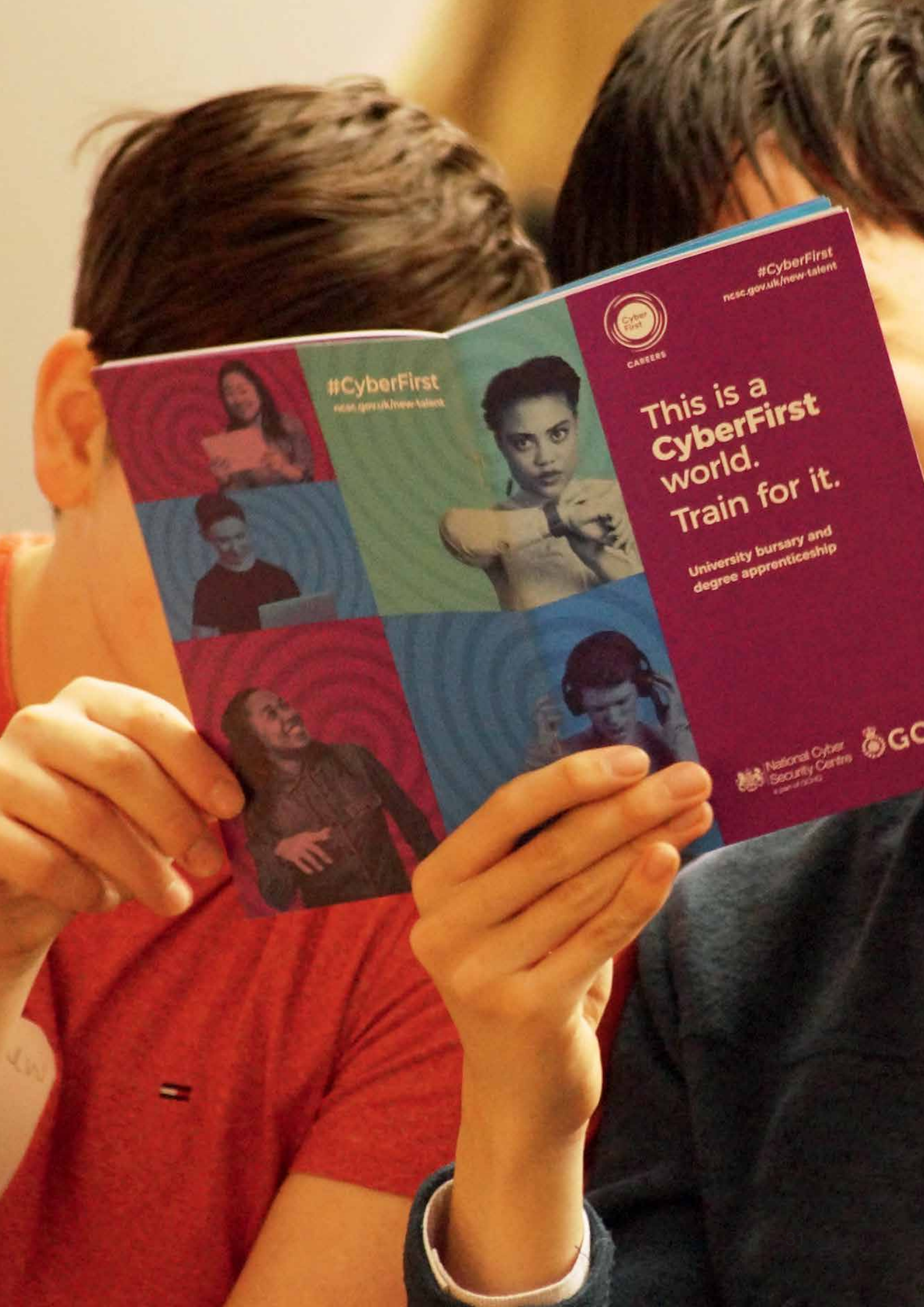
38. サイバー空間を支配するルールをめぐる議論は、今後ますます**大国間の全システム的競争**の場となるだろう。そこでは、開かれた社会に基づくシステムを維持していきたい国と、中国やロシアなど、国家統制の強化をサイバー空間確保の唯一の方法として推進する全システム的競合国との間で、価値観の衝突が発生する。このため、自由でオープンなインターネットには圧力がかかるだろう。国家や、大手テクノロジー企業、その他の行為者が、技術標準とインターネットガバナンスに対して競合的アプローチをとろうとするからである。

39. さらに、**急速に進化するテクノロジー環境の支配をめぐる競争**も、事態を悪化させるだろう。デジタル技術が日常生活やビジネス、インフラに組み込まれていくとともに、一部の技術は社会機能にとって必要不可欠なものとなる。パワーを獲得できるのは、科学技術で戦略的優位に立ち、イノベーションを推進するデータにアクセスできる国となる。そのような国は、他国に影響力を行使し、様々なグローバルスタンダードを自国の経済的・政治的利益に最も適う方法で形成できるようになる。

40. デジタルツイン、量子コンピューティング、大規模自律システム等の**新興テクノロジー**と、それが生み出す情報は、新しい機会とリスクを創出し、攻撃者と防御者の双方に新たなサイバー能力を開放するだろう。それはまさに、暗号通貨がランサムウェア犯罪集団に悪用されているのと同様である。テクノロジー分野のリーダーシップは分散化しており、英国が重要技術のすべてにおいて主権的に能力を開発するのは不可能である。様々な国家と企業が技術標準を自らの利益を推進するための手段としており、重要技術が英国の価値観を共有しない国によって形成されるリスクが生じている。

41. 英国は10年以上にわたって野心的な国家サイバーセキュリティ戦略を追求し、多額の投資を継続的に行って、サイバー分野の世界的リーダーの地位を確立してきた。しかしこれまでの分析からも明らかなように、重大な課題と機会がなお残っている。以下に続くセクションでは、英国の国家的対応について概要を説明する。

[18] 英国政府、National Space Strategy（「国家宇宙戦略」）(2021年)


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

英国の国家的対応

42. このような戦略的環境の中、英国は選択を迫られている。複雑化するサイバー空間において直面する脅威や機会に、単純に対応を続けていくということも可能かもしれない。その場合、過去5年間の進歩を定着させ、可能な限り最も緊急性の高い問題に対処することを目指せばよい。しかしこのアプローチには2つのリスクがある。その一つは、英国のサイバー分野の強みがもつ潜在力を、国の優先課題の追求に十分に活用できず機会を逃してしまうリスクである。そしてもう一つのより深刻なリスクは、テクノロジーの転換点を迎えた時に、英国の経済社会の将来的基盤がすでに競合国や敵対者によって形成されており、自国の安全確保にいっそう努力しなければならなくなるというリスクである。

43. サイバー空間は英国と同盟国、そして敵対国にとっても、国益追求のために根本的重要性をもつようになっている。**このような状況を切り抜けていくうえで、自国の競争的優位の育成は戦略上の至上命題である**と英国政府は判断している。それによって、今日の安全保障を確保するだけでなく、明日の世界を形成し、そこから利益を得ることも可能になるだろう。

英国のビジョン、目標、理念

44. 英国のビジョンは、2030年も引き続き**責任ある民主的なサイバー大国としての地位を保ちながら、サイバー空間の内部およびサイバー空間を通じて国益を保護・増進しつつ国家目標を追求していくこと**である。

45. このビジョンの実現のために、5つの戦略目標を設定した。各目標はサイバーパワーの5つの次元のそれぞれにおいて国力を強化することを目的としている。全体として、英国の価値観と利益を反映するサイバー空間の維持に必要な能力の強化を目指す。この5つの目標（または柱とも呼ぶ）は、英国の活動の指針となる戦略的枠組みを構成する。2025年に向けて取るべき行動については、第2部で各目標ごとに説明する。

- **第1の柱：英国サイバーエコシステムを強化する。**人材とスキルに投資し、政府・学術界・産業間のパートナーシップを緊密にする。
- **第2の柱：レジリエントで豊かなデジタル国家を構築する。**サイバーリスクを削減することによって企業はデジタル技術の経済利益を最大化し、市民はオンラインの安全性と個人データの保護に関する信頼性を享受できる。
- **第3の柱：サイバーパワーに死活的重要性をもつ技術を先導する。**産業の能力を増強し、将来のテクノロジーを確保する枠組みを構築する。
- **第4の柱：より安全で、豊かで、開かれた国際秩序のために、英国のグローバルなリーダーシップと影響力を増進する。**政府および産業界のパートナーと協力し、英国のサイバーパワーの基盤となる専門知識を共有する。
- **第5の柱：サイバー空間の内部およびサイバー空間を通じた英国の安全保障の強化のために敵対者を検知し、攪乱し、抑止する。**英国が持つあらゆる手段を、より統合的、創造的、日常的に活用する。

46. 上記の目標は相互に補強し合うことが意図されている。例えば、国内のサイバーセキュリティとレジリエンスのレベルアップは、国際舞台で積極的な立場をとるための必要条件である。また、英国のサプライチェーンがグローバルであり、国外から現実的脅威を受けていることから、国際的行為者の行動を積極的に形成していかない限り自国の安全は確保できない。さらに、サイバー空間やインターネット、テクノロジーに関するグローバルな議論に影響力を行使できるかどうかは、技術的先端能力を維持し、最重要テクノロジー分野で真の優位を生み出すイノベーションのエコシステムを構築できるかどうかにかかっている。

47. 英国のビジョンの中心にあるのは、**自由でオープンで平和で安全なサイバー空間の推進**である。サイバーパワーに戦略焦点を絞るということは、対立を煽ったり、ゼロサムゲームで勝利を目指すということではない。「統合レビュー」でも明らかにしたように、開かれた社会と経済が繁栄しうる世界は、英国にとっても将来の繁栄、主権、そして安全保障を確保できる世界である。英国はパートナー諸国と協力して、開放的な民主主義という共通の価値観を推進しながら、**サイバーパワーへの責任ある民主的アプローチ**を追求していく。それはつまり、5つの戦略目標への取り組みおいて、以下のような**原則**を適用していくことを意味する。

- 英国は、市民と企業がサイバー空間で安全に活動し、デジタル技術の経済的・社会的メリットを最大化して法的・民主的権利を行使できることを優先課題とする。
- 英国は、オープンで相互運用可能なインターネットを、世界の繁栄と幸福を支える最良モデルとして擁護する取り組みを行い、権威主義的国家による断片化への圧力やインターネット主権の考え方に抵抗していく。

- 英国は、自国のサイバー能力の合法的でバランスの取れた責任ある利用を、明確な管理と国民および同盟国との協力を通じて実施するとともに、サイバー空間で見境のない無差別的行動を取る国に対して責任を追求していく。
- 英国は、サイバー空間の犯罪的利用に対してはあらゆる手段を用いて対抗措置をとり、犯罪的なプロキシ使用者や、犯罪集団を領土内にかくまう国家を非難するとともに、ハイエンドなサイバー能力が犯罪者に拡散しないよう努力を尽くす。
- 英国は、サイバー空間とデジタル技術の未来に関する議論では、インクルーシブでマルチステークホルダー型のアプローチを擁護し、サイバー空間における人権を守るとともに、デジタル権威主義や国家統制へと向かう動きに対抗していく。

英国のアプローチにおける主な変化

48. 英国は様々な分野の戦略を、現行のアプローチを基盤としながら必要に応じて取り組みを強化、拡大、適応させる形で構築していく。本戦略が前戦略「国家サイバーセキュリティ戦略2016-2021」と特に異なるのは、以下の点である。そこには、英国の先進的サイバー大国としての地位を固めるという野心的目的が反映されている。

49. 英国がサイバー分野の最先端に立ち続けるためのコミットメント。政府は今後3年間に、サイバーおよびレガシーITに26億ポンドを投じる予定である。これは、SR20（2020年歳出レビュー）で発表した国家サイバー部隊への大規模投資とは別に実施される。ここには国家サイバーセキュリティプログラムへの1億1400万ポンドの増額投資が含まれる。またこれと並んで、研究開発、情報（インテリジェンス）、国防、イノベーション、インフラ、スキルへの資金の増額も発表しており、これらすべてが英国のサイバーパワーの一端を担うことになる。SR20とSR21（2021年歳出レビュー）で発表したサイバー投資額は、前戦略が約束した5年間の19億ポンドをはるかに上回る。[19]

50. より包括的な国家サイバー戦略である。本戦略は引き続きサイバーセキュリティを最重視するが、それにとどまらず、英国のあらゆる能力を政府内外含めて結集する。特に、サイバー空間を支える重要技術およびインフラにいっそうの重点を置き、英国サイバー企業の国内的成長と国際的競争を支援するとともに、これからのサイバー空間を形成し影響力を行使していくための国際的行動を拡充し、さらには攻撃型サイバーパワーを手段の一つとして統合する。それは真に統合された、国家戦略的アプローチを目指す。また、リーダーシップと調整の責任をそれぞれの国務大臣に幅広く負わせ、英国内4つの自治政府との協力関係も従来以上に緊密なものにする。基盤となるのは政府全体を通じた取り組みの効果的な調整であり、それは英国の主たる強みの一つである。

[19] 財務省、Autumn Budget and Spending Review 2021（「2021年秋期予算及び歳出レビュー」）(2021年)

51. 全社会的な取り組みである。英国が目指すのは、国内諸組織の意思決定に支えられ、またその指針になるとともに、国内外のパートナーとの協力関係強化の基礎にもなる国家戦略的アプローチである。それを実現するには、さらなる努力が必要である。短期的に取るべき行動としては、次が挙げられる。(i) 新しい国家サイバー諮問委員会の設立。民間および第3セクターの上級指導者を招いて政府のアプローチに挑戦し、支援し、助言を行ってもらう場とする。(ii) サイバー部門のイノベーションプログラムを、これまでのようなロンドン中心の大規模なイニシアチブから、地域の産業、イノベーター、法執行機関、学術界と連携して地域レベルで実施されるモデルに転換する。(iii) サイバー部門の労働力の多様化を進める措置をとる。これは、全人口のスキルと能力を活用・育成できることが、英国の安全保障にとって必要不可欠であるとの認識に基づく。本戦略はそれ自体が、北アイルランド、スコットランド、ウェールズの各自治政府と、産業界、法執行機関、規制当局、学術界、市民社会組織、パートナー諸国との協力を通じて得た情報によって策定されている。英国は、このような様々な対話を、本戦略の実施期間中も継続していく予定である。

52. 積極果敢なアプローチによって、サイバー空間に必要不可欠な技術の競争優位を育成し、保護する。「統合レビュー」とそれに続く様々な戦略では、すでにこのアプローチを、AI、量子テクノロジーおよびデータ等の分野でとり始めている。本戦略ではさらに進んで、安全なマイクロプロセッサ設計や、運用技術および暗号技術のセキュリティに関してコミットメントを行う。また、運用技術セキュリティのための国立研究所の設立も発表する。これは最高水準のサイバーレジリエンスを産学連携で構築することを目指す新しい研究施設である。さらに国家サイバーセキュリティセンター（NCSC）の研究能力の拡充も発表する。ここには、マンチェスターの新しい応用リサーチハブ等が含まれ、コネクテッドプレイスやコネクテッド輸送等の分野の新技術に焦点を当てている。本戦略はまた、英国が様々なアプローチのもと、新技術が設計段階からセキュリティを組み込んだ「セキュアバイデザイン」となるよう図り、成果をあげてきたことにも依拠している。このことは、すでに電気通信分野で実施してきたことと同様に、投資を行い、必要に応じて規制や法律を活用しながら、多様性が高く安全かつレジリエントなテクノロジーサプライチェーンを促進していくことを意味する。

53. サイバーセキュリティ推進のための中核的な取り組みを、政府主導で大幅に強化する。英国はこれまで以上の資金を投じて政府のサイバーセキュリティの迅速かつ抜本的な見直しを行い、各省庁のために明確な基準を設けてレガシーITインフラに対処していく。政府の重要機能は、2025年までにサイバー攻撃に対して大幅に強化される予定である。また、公共部門全体を含むすべての政府組織が2030年までに、既知の脆弱性と攻撃手法に対してレジリエンスを獲得できるようにする。また、国民を守り、国民の協力を得ると同時に、できるだけその負担を取り除いていくには、一層の取り組みが必要である。英国はデジタル環境を強化し、国民をサイバー犯罪や詐欺から守るとともに、メーカー、小売業者、サービスプロバイダー、公共部門にはサイバーセキュリティの水準を高める責任を課していく。さらに、サイバーレジリエンスへの民間セクターの関与と投資の水準を引き上げるため、経済全体で規制とインセンティブを調整し、より多くの支援を提供する。加えて、サプライチェーンのリスクもいっそう重視し、組織がサプライヤー由来のサイバーセキュリティリスクを管理できるよう幅広い介入策を試みるとともに、サプライチェーン全体にベストプラクティスを浸透させていく。

54. 敵対者を混乱させて抑止し、サイバー空間における英国の利益を保護・増進するために、統合された持続的キャンペーンを展開する。このようなキャンペーンは、政府全体の外交的、政策的、および運用上の様々な手段をこれまで以上に広範に活用するものとなる。そしてこれを大きく支えるのが国家サイバー部隊（NCF）の設立と拡充であり、同部隊は今後ランカシャー州サムルズベリーに拠点が置かれる。NCFが有する、国家および非国家主体の脅威を破り、国家安全保障上の広範な利益を支えていく能力は、これまで以上に日常的に活用される。英国のキャンペーンはまた、国、地域、地方レベルの法執行に関わる高水準の機能に多額の新規投資を行うことで、利益を得られるだろう。これにより、ランサムウェアや、革新性を増すサイバー犯罪の深刻な脅威に対処していくことが可能となる。また、英国の自律的なサイバー制裁体制および帰属プロセスも引き続き活用し、敵対者にコストを課すとともに、悪質で見境のない攻撃を非難していく。

55. サイバーパワーを英国の外交政策の中心に据え、戦略のあらゆる部分で国際協力が必要であることを認識する。英国は中核的な同盟関係を強化して、これまで以上に広範な国々と協力関係を築き、デジタル権威主義の広がりに対抗していく。今後数年間は、パートナー諸国を支援する国際プログラムへの投資を増やし、それらの国のレジリエンスの構築およびサイバー脅威への対抗能力の強化を手助けしていく予定である。また、国内におけるあらゆる強み、例えば、事業運営や戦略上のコミュニケーション関連知識や、ソートリーダーシップ、様々な取引関係、産業界とのパートナーシップ等をより効果的に活用し、国際的目標を追求していく。

役割と責任を英国全体で担う

56. 英国の戦略の中心にあるのは、サイバーへの全社会的アプローチである。必要なのは、永続的でバランスのとれたパートナーシップを官民・第三セクター横断的に構築して、それぞれが国家的取り組みの中で重要な役割を果たしていくことである。

国民

57. 本戦略は国民のサイバーセキュリティ負担をできる限り取り除くことを目的としているが、全員が引き続き重要な役割を担っていかなければならない。政府は、サイバー攻撃を未然に阻止する努力を最大限に実施するが、脅威の行為者の中には、そのような政府の保護を回避する方法を見つけてしまう者も現れるだろう。貴重な資産のセキュリティを改善するために、すべての人が実世界および仮想世界で行動をとることができる。[20] すなわち、個々人が責任をもって、ハードウェア（スマートフォンやその他のデバイス）だけでなく、生活や仕事で自由や柔軟性、利便性を与えてくれるデータ、ソフトウェア、システムを保護するため、あらゆる妥当な手段を講じなければならない。これを支援するために、政府は技術的に正確で、タイムリーで、実行可能なアドバイスを提供する。また、市民社会組織や各種コミュニティグループもまた、人々がサイバーリスクを理解し自衛できるようにする支援において重要な役割を担う。例えば多くのチャリティ団体は、脆弱な人々のために的を絞った支援やアドバイス、啓発活動を行う。

[20] 政府はサイバーアウェア（Cyber Aware）において、オンラインを安全に利用するためのアドバイスを提供している。

企業と団体

58. 企業と団体は、サイバーリスクを効果的に管理し、サイバーレジリエンスを高め、顧客やサービス利用者をサポートする責任がある。これらの組織は、事業運営やイノベーション、成長のためにデジタル技術やオンラインサービスに依存する度合いがますます高まっている。それによってサービスが向上する一方、新たなリスクや課題も生じている。例えば、責任を負うべき個人情報やデジタル資産が絶え間なく増加しており、そのようなデータや資産の保護を、サービスを維持しつつ行っていかなければならない。それを怠る組織は評判と経済面で深刻な影響を被り、顧客にも損害が及ぶ可能性がある。特に必要不可欠なサービスの事業者や重要デジタルサービス（クラウドサービス等）のプロバイダーは、現実的サイバーリスクに対処して、ネットワーク・情報システム規制（「NIS規制」）が定める義務を果たすという特定の責任を負う。NCSCはアドバイスとガイダンスを提供し、すべての企業と組織が情報、資産、システムを保護できるよう支援する。また情報コミッショナー事務所（ICO）は、英国一般データ保護規則に基づいて、組織に対してサイバーセキュリティの義務に関するアドバイスを行う。

サイバーセキュリティセクターと主要テクノロジー企業

59. 英国の成長部門であるサイバーセキュリティセクターは、英国が直面する新種のサイバー脅威および課題に対応する重要な役割を担う。接続可能な製品の急速な普及と、企業や組織で加速的に進むデジタル変革は、同セクターにとって成長とイノベーションの機会であり、新たなサービスや製品を生み出している。本戦略は、政府がどのようにして英国のサイバーセキュリティセクターの成長を継続的に支援し、パートナーシップの維持・強化を通じて同セクターの能力と専門知識から利益を得ることができるかを説明する。また、英国全体の技術的専門知識やノウハウをフルに活用するために、学術界や、広範な技術コミュニティ、民間企業間の間の幅広いパートナーシップを強化していく。

60. デジタルサービスを提供する主要テクノロジー企業は、英国企業と組織が安全に活動できる環境を確保するうえで重要な役割がある。特に、様々な活動を統合するマネージドサービス・プロバイダーやプラットフォームビジネスがこれに当てはまる。それらの企業は、提供するサービスを標準初期設定でセキュリティを組み込んだ「セキュアバイデフォルト」にして、顧客による保護措置に過度に依存しないようにする必要がある。また各企業とも、自社のサイバーレジリエンスを優先課題にするという特定の責任を負う。クラウドやオンラインサービスへの企業、政府、一般社会の依存が高まるにつれ、他にはない新たな脆弱性と相互依存性が生じている。

政府

61. 英国政府は、きわめて巧妙な脅威を理解し、法律を制定・施行し、国家的基準を設定し、敵対的行為者の脅威に対して攻撃型のサイバー作戦の実施を含めて対抗するのに必要となる情報（インテリジェンス）の結集という、他とは異なる独自の機能をもつ。本戦略のもとで英国は、国家のサイバー能力強化のために投資を実施していく。政府諸機関と公共部門もまた、自らのネットワークとシステムを保護する責任を負う。重要データを保有するサービス提供者として、政府は、情報資産を保護するための厳格な措置をとる。そして最終的に、政府は、国民、企業、組織がオンラインで身を守るためにすべきことについて助言と情報を与えるという重要責任を負う。ここには、我々全員を守るために主要企業および組織に順守してもらうべき様々な基準を、必要に応じて設定することも含まれる。

62. サイバー政策のほとんどの分野と、本戦略で取り上げる対策の大部分は、国家安全保障、外交・防衛、電気通信、製品規格・安全、消費者保護等、それぞれの所轄官庁の専任事項に関わる。しかし本戦略の策定と実施は、**北アイルランド、スコットランド、ウェールズの各自治政府**が提供する情報や、行動、投資にも依存している。この点は特に、各自治政府の教育、警察や、それぞれの公共部門を含む特定重要セクターのサイバーレジリエンス等、本戦略の「エコシステム」と「レジリエンス」の2つの柱に関わる政策分野について当てはまる。英国の4つのネーション間の調整と協力は、英国全体で最大限の効果を実現するのに不可欠である。そのためには、内閣府を始めとする英国政府各省庁が、ウェールズ、スコットランド、北アイルランドの担当部署と定期的かつ早期に関わり、優先事項や計画について情報を共有する必要がある。そうすることで重複も避けられ、公的資金を最大限に活用できる。各自治政府は引き続き、それぞれ独自のサイバー戦略と計画を、英国政府の本戦略と整合させつつ策定していく。

国家サイバーセキュリティセンター

「英国を、オンラインで安全に生活し仕事ができる国にするための機関である」

国家サイバーセキュリティセンター（NCSC）は、GCHQの一部を構成する組織として、2017年に正式に発足した。サイバーセキュリティ環境を管轄する国家機関として、知識の共有、全システム的脆弱性への対応、国家の重要サイバーセキュリティ問題におけるリーダーシップの提供を行っている。[21] NCSCの設立で政府の運営構造が簡略化され、国家レベルのサイバーインシデントへの対応能力が向上した。また、革新的なデジタルサービスの配備を開始し、組織と個人がオンラインの安全性を自動的に享受できるようになった。

英国は、NCSCが今後10年間の課題に十分に対応できるよう、その活動を支える持続的能力と特質を明確化し、継続的に資金を提供するとともに、これまでの経験から国家規模で最大限の効果を発揮できると考えられるケースに絞ってこれを利用している。

NCSCの活動基盤となる持続的な能力と特質は以下の通りである。

- 英国が必要とするサイバーセキュリティ領域および特殊分野の世界水準の技術的専門知識。
- 英国の利益に対する現実的および潜在的なサイバー脅威（意図と能力）についての比類ない理解。
- サイバーセキュリティ目標を実現するために、英国の国家安全保障能力および権限のすべてにアクセスできること。
- 学術界、産業界、国際パートナーと連携して、サイバーセキュリティコミュニティに直接アプローチできること。
- 英国の利益の安全とセキュリティをグローバルに確保するのに不可欠な、暗号能力およびサービス。

新戦略に基づくNCSCの主な責務は以下の通りである。

- **英国のサイバー被害を減らすために直接行動をとること。**デジタルサービス（アクティブサイバーディフェンス等）を通じて大規模に保護を提供し、技術変革を促進し、国家的重大性をもつサイバーインシデントへの対応を管理するとともに、国家サイバー軍（NCF）とともに敵対者のサイバー作戦に直接対抗する。

[21] 英国政府、National Cyber Security Strategy 2016 to 2021(「国家サイバーセキュリティ戦略 2016-2021」(2016年): パラグラフ 1.9

- **英国社会のあらゆる部分に自衛のための支援を行うこと。**すべての国民、企業、組織が自衛のために利用できる専門知識と独自情報をテーラーメード方式で提供し、英国をオンラインを利用するすべての人にとってより安全な場所にする。
- **英国政府の政策および規制に役立つよう、サイバーセキュリティの最重要課題に関する技術的インプットを提供する。**中央政府の政策責任者に、NCSCの中核能力で得られる権威ある技術的インプットおよび脅威評価を提供し、国民、組織、利益をデジタル的に安全に保つための政策・規制の策定および実施を支援する。
- **英国に主権的能力を提供する。**NCSCの国家暗号キーセンター（National Crypt-Key Centre）が、英国軍や国家安全保障関係機関にとって枢要となる重要情報およびサービスを、特に能力の高い敵対者からの攻撃対応も含めて保護する。
- **サイバースキルと投資の成長を支援する。**あらゆるレベルのサイバー教育に技術的支援を提供し、産業界を巻き込んで支援するとともに、サイバーセクターへの投資を促進する。

NCSCはまた、本国家サイバー戦略の目標に向けた**進捗評価**において、NCSCアセスメント（英国が有する編集に依存しないサイバー評価機能）を通じて貢献する。

国家サイバー部隊

2020年に設立された国家サイバー部隊（NCF）は、英国と同盟国に危害を及ぼす者を撃退し、混乱、弱体化させてこれに対抗し、国の安全を守り、さらに国内外の利益を保護し増進するための、サイバー空間の内部およびサイバー空間を通じた活動に責任を負う。NCFは、国防および情報機関からのほぼ同数の人員で構成されており、それぞれの専門知識、資源、権限を単一の指揮系統のもとに結集している。地理的拠点はランカシャー州サムルズベリーに置かれる。

NCFは、国防や、英国経済の健全性、重大犯罪防止の支援といった国家安全保障に関わる幅広い成果を提供している。その活動は、国家的行為者と非国家的行為者の両方を対象として、戦術的なものから戦略的なものまで多岐にわたる。活動は大きく3つに分類される。

- テロリスト、犯罪者、外国国家が英国や他の民主主義社会に危害を加えるためにインターネットを使って国境超越的に活動することから生じる脅威に対抗すること。
- サイバー空間でデータおよびサービスの機密性、完全性、可用性を阻害する脅威に対抗すること（サイバーセキュリティの支援等）。
- 英国の国防活動に貢献し、外交政策アジェンダの実現を支援すること（例えば人道的危機に介入して民間人を保護する等）。

NCFの活動は、個人や集団に影響を与えたり、オンラインや通信システムを混乱させ、物理的システムの運用を低下させたりするために使用されることもある。この種の活動は攻撃型サイバー（OC）とも呼ばれる。

NCFの活動は、1994年情報サービス法や2016年捜査権限法を含む確立された法的枠組みに沿って実施されている。英国はこれまで、能力の開発と配備を（適用可能な場合は武力紛争法も含む）国際法に従って行うことを明確にしてきた。英国の活動は、閣僚の承認、司法の監督、議会の審査のもとにあり、サイバー活動に関する英国のガバナンス体制は世界最強に数えられている。

英国は個々のサイバー作戦について日常的に公表することはないが、NCFが実施しうる作戦活動としては以下が挙げられる。

- テロ集団の計画実行を阻止するために、同集団の指揮統制通信を不能にし、過激派メディアの情報流布を制限する。
- 英国軍に危害が及ぶリスクを削減するため、敵対者の兵器システムを弱体化させる。
- 民主主義と、自由・公平で開かれた選挙を擁護するため、その弱体化を狙う外国国家の組織的な偽情報キャンペーンに対抗する。
- 犯罪集団が活動から利益を得るのを防止するため、オンラインプラットフォームやサービスの利用を妨害する。
- 国際的な制裁措置の執行を手助けするため、それを回避しようとする動きを阻止する。
- 英国や他の国々をサイバー攻撃から守るため、敵対者がサイバー攻撃に使用するインフラを破壊する。
- 人道的危機にある民間人を保護するため、それらの人々が重要情報にアクセスする能力を維持していく。

NCFは、サイバー空間の内部およびサイバー空間を通じた効果的作戦のための国家的研究センターである。上記能力をその他の能力とともに開発、統合、利用して、効果的実現のために最適化していけるよう英国の能力を変革していく。

法執行機関の全国サイバー犯罪対策ネットワーク

「国家サイバーセキュリティ戦略2016-2021」に基づき設立された法執行機関の全国サイバー犯罪対策ネットワークは、サイバー犯罪への完全統合された対応を展開している。個人、組織、またはセクター全体に対するあらゆる形態のサイバー攻撃に対し、情報（インテリジェンス）主導で対応する態勢を整えており、全国規模のシステムとして、国、地域、地方レベルで運用されている。また被害者のケアの提供や、企業や人の保護と迅速な回復を支援するとともに、加害者への刑事司法の適用を追求している。

国家犯罪対策庁（NCA）の国家サイバー犯罪対策ユニット（NCCU）は、対応に関して国家レベルのリーダーシップをとり、調整を行う機関である。イングランドとウェールズの9つの警察管轄区域にある専門的な**地域サイバー犯罪対策ユニット（RCCU）**のネットワークから支援を受けつつ、スコットランド警察と北アイルランド警察、さらにはロンドン警視庁のサイバー犯罪対策ユニットとも連携している。

さらにこれを補完するのが、43の警察部隊それぞれに設置されている専門的な**地方サイバー犯罪対策ユニット（LCCU）**で、これは地域コーディネーターを介して調整されている。このような地域および地方レベルのサイバー犯罪対策ユニットは、犯人を捜索し、企業や被害者が攻撃から身を守る支援を行うとともに、パートナー機関と協力して脆弱な個人がサイバー犯罪に引き込まれるのを防止することができる。

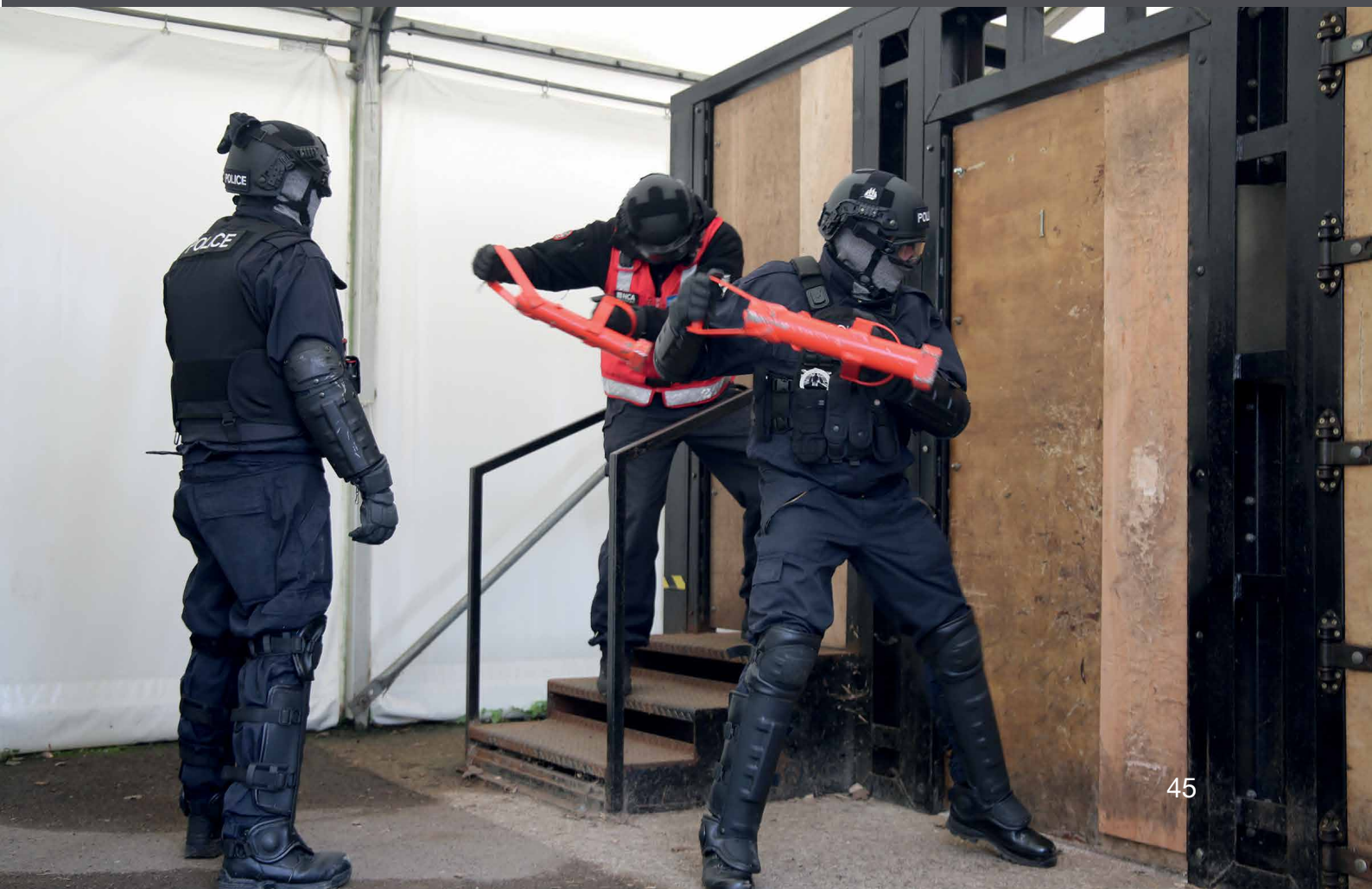
ロンドン市警察が主催する**アクションフロード**は、犯罪報告、トリアージ、分析を一元的に行う。特に深刻または複雑なケースは、その後NCAと地域ネットワークに照会され追及されるが、その他のケースは地元の部隊に送付される。ロンドン市警察はまた、**経済犯罪被害者ケアユニット**等を通じた被害者支援の調整を行う。

様々なシステムが、フォレンジック、インテリジェンス、データ共有の各新機能と統合されて単一のプラットフォームを構成する。そのため、国と地域それぞれのユニットがあらゆる専門ハイエンド能力および開発途上のツールにアクセスできる。

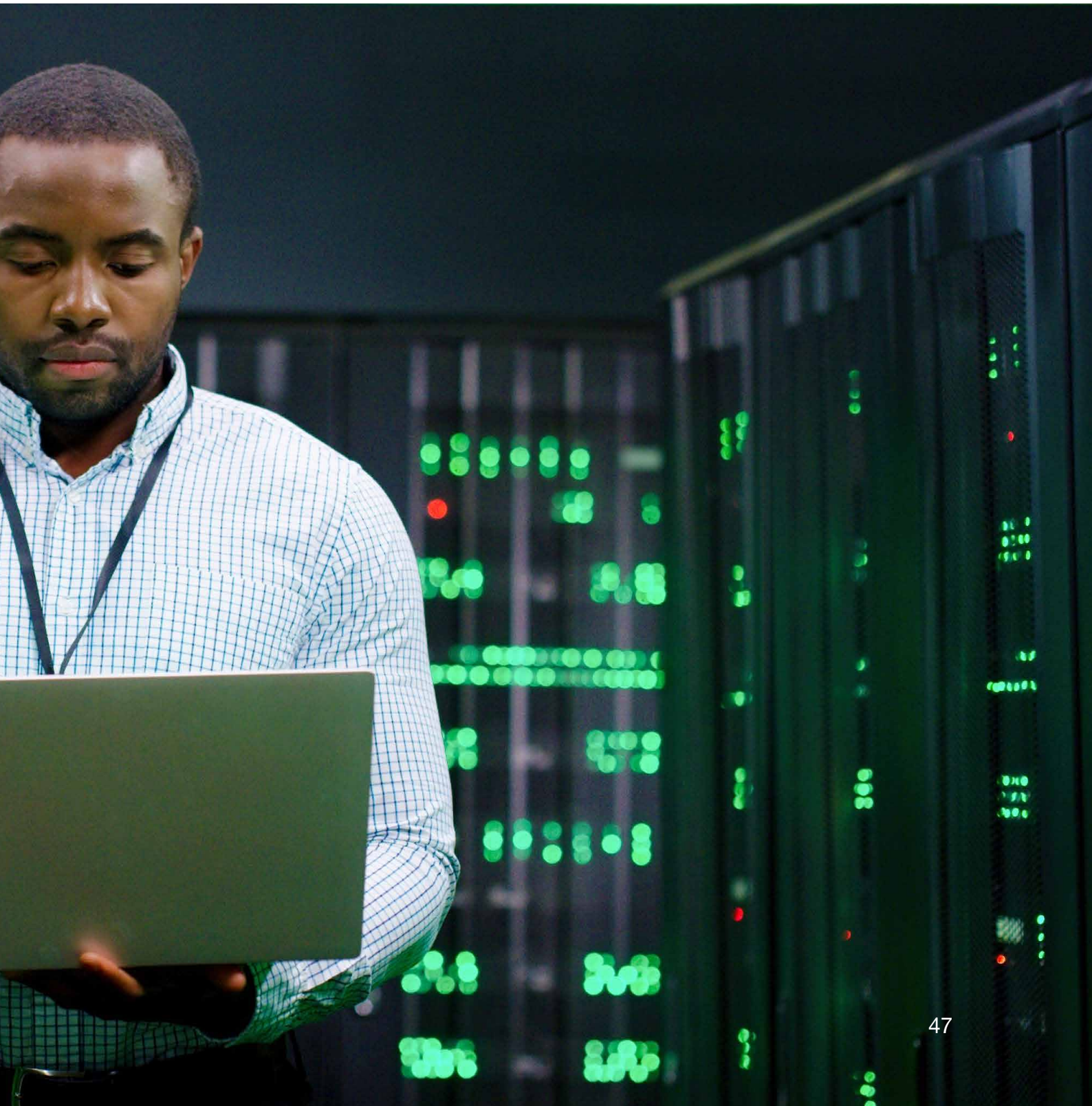
ここには、特に犯罪と国家的脅威の混合形態に対応するため、安全保障および情報関連機関と効果的に連携、協力する能力も含まれる。これらの能力は、「一気に、かつ全国的に構築するのがサイバー犯罪対策ネットワーク全体の利益になる」という理念に従ったものだが、地方のサイバー犯罪対策ユニットもまた地域コーディネーターを通じてこれを利用することが可能である。このような全システム型アプローチにより、サイバー犯罪の脅威への対応はすでに大幅に強化されている。

法執行機関のサイバー犯罪対策ネットワークは、サイバー空間における悪質な活動への刑事司法対応を、国際的、国内的、地域、地方のどのレベルの脅威であるかにかかわらず引き続き推進していく。またそれを補完するものとして様々な破壊的手段があり、例えば以下のようなものがある（なおこれらに限定されない）。

- 特殊ハイエンドの捜査的および破壊的なサイバー能力の開発。
- NCAの広範な国際ネットワークの活用を通じた、情報（インテリジェンス）と証拠に基づくパートナー諸国の介入支援。
- 犯罪集団が活動から利益を得られないようにするための、犯罪市場および支援サービスの利用妨害。
- 英国と他の国々をサイバー犯罪から守るための、犯罪に使用されるインフラの弱体化および破壊。
- ハイレベルの犯罪者に対する制裁活動およびパブリックアトリビューション（public attribution）への貢献。
- 暗号通貨やその他の資産をサイバー犯罪の収益として押収。



第2部：
戦略の実施



第1の柱：
英国のサイバーエコシステム

英国のサイバーエコシステムを強化する

63. 英国が本戦略を成功させるには、適切な人材、知識、パートナーシップを確保しなければならない。多様で技術スキルの高い労働力、活発な研究コミュニティ、国際競争力のあるサイバーセクター、そして重要技術分野でのリードを可能にする地域に根差したイノベーションのエコシステムのすべてを、政府、産業界、学術界の力強いパートナーシップの基盤の上に築いていく必要がある。

64. サイバーエコシステムの成長は、政府の介入策に依存しない自立的なものになる必要がある。本戦略の遂行を通じて、スキルやイノベーションプログラムに資金提供する、個別適応中心の一元管理されたアプローチから、より持続可能で、全システム的かつ地域レベルのアプローチへの移行が実現するだろう。英国は、政府が進める幅広いスキルおよび教育制度の改革に基づいて、より多くの人がサイバー分野のキャリアに必要なスキルを身につけられるよう支援し奨励していく。また、サイバー分野の労働人口の多様性を高めるべく、多種多様な具体策を優先的に実施していく。国民全体の才能とスキルを活用するこの政策は、サイバー分野の仕事やキャリアの機会を国民に広く開放するばかりでなく、国家安全保障にとっても重要な使命である。さらに、サイバーセクターの成長が英国全土に利益をもたらすようにしていく。現状では同セクターの雇用の45パーセント、対英投資の85パーセントがロンドンとイングランド南東部に集中しており、是正が必要である。[22]

65. 全体として、政府はより戦略的な役割を担い、産業界のリーダー、学術研究者、イノベーター、法執行機関、国家安全保障コミュニティとその他の協力者を一つにまとめて、英国のサイバー脅威に対するレジリエンスを高めていく。また、英国が将来の脅威から身を守るのに必要な能力を確保できるよう、政府のあらゆる手段を用いて、学校のサイバー教育の拡充から経済的規制によるレベルアップにいたるまで、サイバーエコシステムを力強く支援していく。

[22] デジタル省、Cyber Security Sectoral Analysis 2021（「サイバーセキュリティセクター分析 2021」）(2021年)

目的1：サイバーへの全社会的アプローチの支援に必要な構造、パートナーシップ、ネットワークを強化する。

66. サイバーパワーは全社会的アプローチを必要とする。英国の競争優位は、国全体で人材を育成・活用し、公共セクター、産業界、学術界のすべて及ぶ適切な人材を適切な方法で協力させ、サイバーコミュニティ全体をまとめあげることで実現するだろう。そのためには、真に統合された成果重視のパートナーシップを産業界と形成し、北アイルランド、スコットランド、ウェールズの各自治政府と密接に協力しつつ国内各ネーションおよび地域のすべてに及ぶ広範な地理的アプローチを確保して、サイバーパワーがもたらす格差是正の機会を掌握しなければならない。英国は2025年までに以下のことを実現する。

67. 国家のサイバーに関するより包括的で戦略的な対話を産業界、学術界、国民とともに行う。そのために、上級の国家サイバー諮問委員会を新たに設立するとともに、サイバー成長およびレジリエンスのための様々なパートナーシップのネットワークと、サイバーセキュリティ研究・教育の拠点となる卓越研究センターを活用する。

68. より統合され効果的な地域サイバーネットワークを英国全土に構築する。これにより、政府、企業、学術研究機関のパートナーシップを強化し、各セクターの成長と企業のレジリエンスを支援することができる。政府は、地域のサイバークラスターや、新設の英国サイバークラスターコラボレーション(UKC3)、各地に次々と設立されているサイバーイノベーションセンター、サイバーレジリエンスセンターと協力して、地域の企業、卓越研究センター、法執行機関の間の連携を強化してく。

69. これらの施策の基盤となるのは、国家サイバーセキュリティセンター（NCSC）と関連機関の間の協力関係や、政府省庁、様々な公共機関、それらが代表する各経済セクター（CNIや規制当局を含む）の間の協力関係といった既存の幅広い関係と、政府が産業界全体およびデジタル・テクノロジー分野の各セクターとの間で行う広範な対話である。

スコットランドIS サイバー責任者
シアラ・ミッチェル

スコットランドのサイバークラスター責任者、およびUKC3役員も兼任。

「スコットランドのサイバークラスターは、スコットランドのサイバーセキュリティコミュニティの支援に重要な役割を担ってきました。近年、クラスターのマネジメントに関するスコットランドの専門知識と活発なサイバーセクター構築の機会について、理解が深まっています。クラスターの価値がますます認識されている現在、英国の新しいサイバークラスターコラボレーションにおいて、エコシステム開発主任として中心的役割を担えることを嬉しく思っています。UKC3で重点的に扱うのはコラボレーションとイノベーション、そしてスキル開発であり、これが英国サイバーセキュリティセクターの成長を支えるプラットフォームになっています。」

サイバー組織（ロケーションは概略です）

英国サイバークラスター

1. ブリストル&バース・サイバー
2. サイバー・ノース
3. サイバー・ウェールズ
4. CyNam（サイバー・チェルトナム）
5. イーストオブイングランド・サイバーセキュリティクラスター
6. ミッドランズ・サイバー
7. スコットランドIS・サイバー
8. サウスウェスト・サイバーセキュリティクラスター
9. ヨークシャー・サイバーセキュリティクラスター
10. NIサイバー（北アイルランド）
11. ノースウェスト・サイバーセキュリティクラスター
12. ウェストオブイングランド・サイバークラスター

サイバーセキュリティ教育（CSE）分野の卓越研究センター（ACE）

GCHQ / NCSCの拠点

サイバーセキュリティ研究（CSR）分野のチェンジ卓越研究センター（ACE）*

自治政府の組織

* 赤い点と黒い線の組み合わせは、CSEとCSRの両ステータスをもつことを意味する

1 ノースイースト・ビジネスレジリエンスセンター

2 ノースウェスト・サイバーレジリエンスセンター

3 イーストミッドランド・サイバーレジリエンスセンター

4 ウェストミッドランド・サイバーレジリエンスセンター

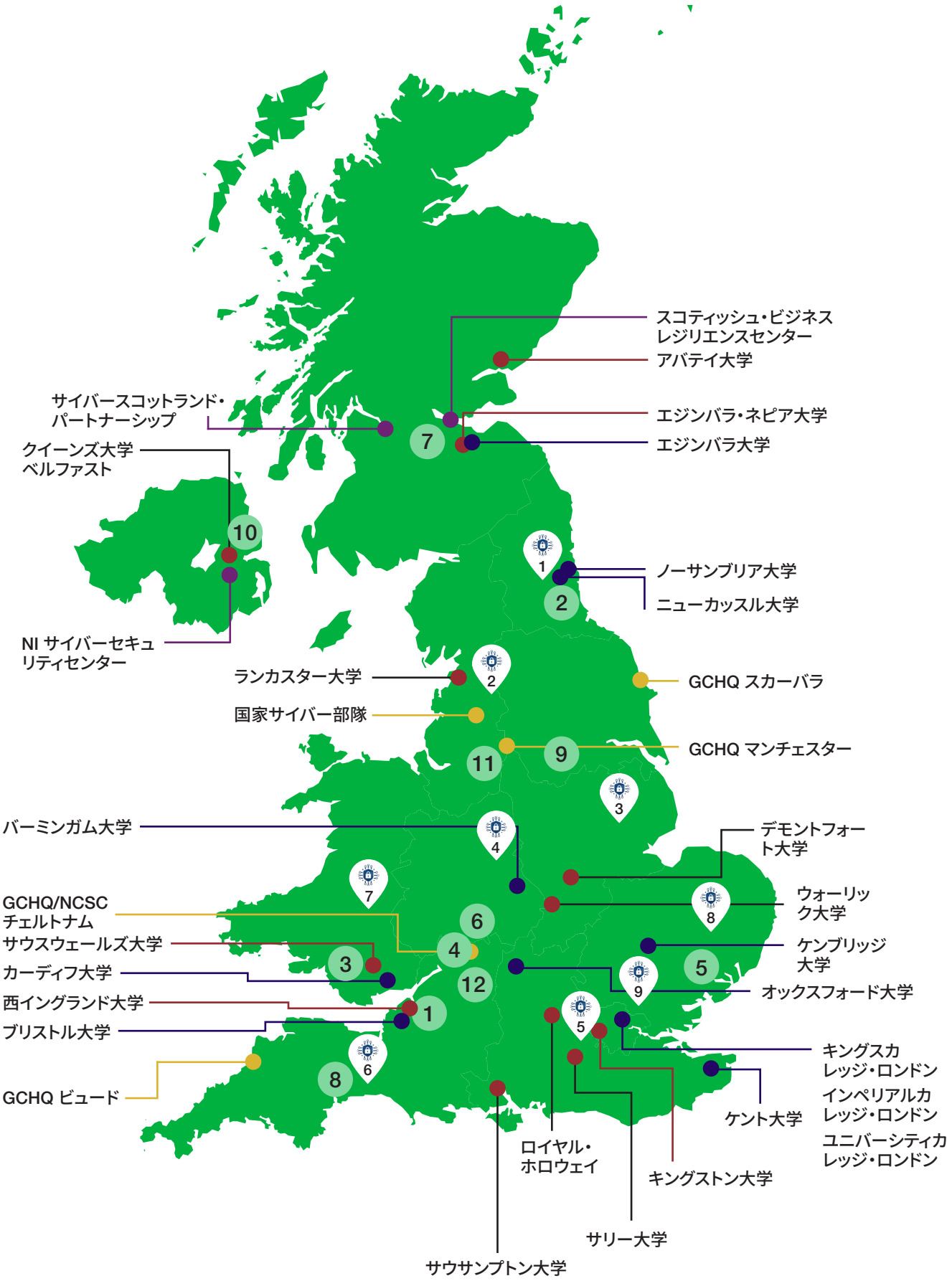
5 サウスイースト・サイバーレジリエンスセンター

6 サウスウェスト・サイバーレジリエンスセンター

7 ウェールズ・サイバーレジリエンスセンター

8 イースタン・サイバーレジリエンスセンター

9 ロンドン・サイバーレジリエンスセンター


スコティッシュ・ビジネス
レジリエンスセンター
アバテイ大学
エジンバラ・ネピア大学
エジンバラ大学
サイバースコットランド・
パートナーシップ
クイーンズ大学
ベルファスト
NI サイバーセキュ
リティセンター
ノーサンブリア大学
ニューカッスル大学
ランカスター大学
国家サイバー部隊
GCHQ スカーバラ
GCHQ マンチェスター
バーミンガム大学
デモントフォー
ト大学
GCHQ/NCSC
チェルトナム
サウスウェールズ大学
カーディフ大学
西イングランド大学
ブリストル大学
ウォーリッ
ク大学
ケンブリッジ
大学
オックスフォード大学
キングスカ
レッジ・ロンドン
インペリアルカ
レッジ・ロンドン
ユニバーシティカ
レッジ・ロンドン
ケント大学
GCHQ ビュード
ロイヤル・
ホロウェイ
キングストン大学
サリー大学
サウサンプトン大学

目的2：
あらゆるレベルで国家のサイバースキルを強化・拡充する。ここには、世界トップレベルの多様なサイバー専門職へと将来世代の人材を育成することも含まれる。

70. 英国の意欲の中心にあるのは、高スキルの人材をサイバー労働力へと持続的かつ多様に供給することである。それによりデジタル経済の中核的要素を確保できるとともに、イノベーションと新しいアプローチの開発が可能になる。そしてこのことは、公共部門全体の専門性を認識して保持し、法執行や国家サイバー部隊（NCF）を含む国防・安全保障の能力の向上を通じて模範的にリードするという英国の目的を支えることになる。本戦略の他の部分と同様に、教育・スキルといった分権事項に関しては、英国政府のイニシアチブに関して国全体で一貫したアプローチが実施されるよう、スコットランド、ウェールズ、北アイルランドの各自治政府と協力していく。英国は2025年までに以下のことを実現する。

71. サイバー労働力として必要なスキルを持つ人材を大幅に増やす。英国の4つのネーション全体で進行している取り組みを基盤として、国民と雇用主のニーズに応える教育・スキル政策を実施する。そのための方法は多数あり、例えば、16歳以上を対象としたサイバー労働力に必要な訓練プログラムの拡大、サイバーセキュリティ分野の様々なスキルアップ合宿への資金提供、技術研究所プログラムの全国展開、大学生を対象としたサイバーファースト奨学金制度の継続等が挙げられる。基盤となるのは、2030年までに16歳以上の教育と訓練の大部分を、雇用者視点で強化された基準に合わせていくという政府の取り組みである。これらは英国サイバーセキュリティ会議とともに広範なサイバーコミュニティに向けて策定され、実習制度、Tレベル（高技能職業訓練課程）、および新しい高等技術資格を支えるものとなる。その際、雇用主が資格と訓練の設計および開発において中心的役割を果たすことが保証される。

72. 質が高く、確立され、広く認められた、体系的なサイバーセキュリティ専門職。勅許団体である英国サイバーセキュリティ会議が、世界をリードするサイバーセキュリティ・ボディオブナレッジ（CyBOK）に基づいて、サイバーキャリアの職業基準とルートを確立する。また、これらの基準を職業全体に定着させ、卓越性と専門性がサイバー労働力全体で明確かつ一貫して認識されるように、法律を含めてあらゆる政府の手段を検討していく。

73. 多様性の高いサイバー労働力。英国内の少数派グループや不利な立場にあるコミュニティの出身者がサイバー分野の職業に就いて活躍できるよう、より効果的なサポートを提供する。例えば、サイバー労働市場への女性の進出の支援や、少数派グループがハイレベルのキャリアを実現できるよう支援する特定の介入策等、方策は多岐にわたる。また、英国の主要プログラムであるサイバーファースト（CyberFirst）の様々な課外活動の成功も基盤として活用していく（例えばサイバーファースト女子学生コンペティション）。さらに、いわゆる落ちこぼれの若者を違法なサイバー活動から引き離し、その才能と熱意を活かせるポジティブな機会を与えることを目的として、国家犯罪対策庁のプログラムであるサイバーチョイス（Cyber Choices）を通じて教育やキャリアの機会を増やしていく。

74. 高スキル人材を、国内教育制度を通じて安定的かつ多様に輩出する。英国は、これまでよりも多くの若者がテクノロジー分野のキャリアを目指すよう、教育を通じて奨励・支援していく。例えば、GCSEまたはスコットランドの相当資格試験でコンピューターサイエンスを選択し、イングランドのTレベルのような生涯教育や実習制度、高等教育機会へと進む学生の数の増加と多様化を進めていく。また、イングランドの教師のスキルアップのために全国コンピューター教育センター（NCCE）を活用し、多くの学生の関心喚起に役立つリソースや能力開発の機会を利用できるようにする。

75. 政府が必要なサイバー専門職を特定、採用、訓練し、保持できること。サイバー専門職の主要雇用主である政府と公共部門は、上記の措置を支援し構築しながら範を示していく必要がある。英国政府は、公共部門全体で一貫性の高い効果的アプローチをとるとともに、公務員や上級指導者のスキルアップと、NCF、NCSC、法執行機関を含む国防・安全保障分野の能力強化のために具体策を講じていく。ここには、サイバーファストストリーム（Cyber Fast Stream）を拡大し、サイバーセキュリティ実習制度の拡充を通じた若年人材への投資や、NCA内の専門スキルプログラムの支援（例えば、大学院生やインターンの受け入れ、テーラーメードのニューロダイバーシティ・プログラム、夏期多様性プログラム等）が含まれる。また、学術界、産業界、パートナー諸国との協力のもと、ディフェンスサイバースクール（Defence Cyber School）を防衛型・攻撃型サイバー訓練を広範に提供するディフェンスサイバーアカデミー（Defence Cyber Academy）へと拡大し成果を上げたことも基盤としていく。

英国サイバーセキュリティ会議

2021年3月に発足した英国サイバーセキュリティ会議（UK Cyber Security Council）は世界初のサイバーセキュリティ職業団体である。その使命は、専門職を代表する声として、サイバー人材の成長と、この分野に幅広く存在する資格、認定、学位に明確性と体系性を与えることにある。これは重要な一歩である。サイバー専門職を、技術的・非技術的な専門知識と経済全体の専門職を組み込んで、医学や法律などのより確立された専門職と同様の幅を持つものとして認識しているからである。

同会議の目的は次の4つである。

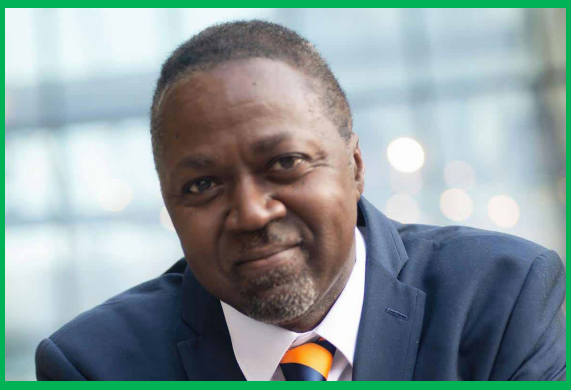
- ソートリーダーシップと職業基準：サイバーセキュリティ専門職を定義する基準の策定および合意のための作業を主導する。
- キャリアと学習：雇用主とキャリアを決定する個人を支援し、サイバーセキュリティのスキル、専門的能力開発、認知に関するアドバイスを提供する。
- 職業倫理：実務専門職および組織自身がサイバーセキュリティ分野の倫理的実践を実証するための指針を提供する。
- ダイバーシティとインクルーシビティ：サイバーセキュリティ専門職を、年齢やバックグラウンドに関わらずすべての人に開かれたキャリアとして推進し、この分野への参入や昇進を阻む障壁を取り除いていく。

同会議は、本戦略のライフサイクル全体を通じて、専門的権威としての信頼性および持続可能性の促進・確立を目指す。また、既存の専門機関や認証機関との幅広い協力のもと、新規参入者、既存の実務家、雇用主のいずれに対しても昇給・能力要件を明確にすることができる専門組織を特定し、権限を与える。

2021年11月、英国サイバーセキュリティ会議は女王より勅許を与えられた。これにより、様々な専門性をカバーするサイバーセキュリティ専門職が初めて公認資格の地位を得た。

職業基準とキャリアパスを、政府、国防、法執行機関を含むサイバーエコシステム全体に組み込むには、なお多くの取り組みが必要である。これに関してサイバーセキュリティ会議は、若者や転職者がサイバー分野のキャリアを検討するよう支援しつつ、重要な役割を果たしていく。

英国サイバーセキュリティ会議 CEO　サイモン・ヘップバーン



私の仕事は、英国サイバーセキュリティ会議を、サイバーセキュリティ専門職を代表する団体として推進していくことです。当会議は、英国のサイバーセキュリティ専門職の自主規制団体です。英国をオンラインで生活し働くのに最も安全な場所にするために、業界を一致団結させ、サイバーに関する全国的に認知された基準を策定、推進、管理することを目的としています。結成プロジェクトの成果を受けて2021年3月に正式に発足し、現在、会員を募っています。国家サイバー戦略は、個人や組織がこの専門職をさらに発展させていくうえで決定的な重要性をもっており、当会議は重要な調整役を果たしています。

目的3：
持続可能で革新的、かつ国際競争力を持つサイバーおよび情報セキュリティセクターの成長を促進しつつ、政府や経済全体のニーズに応える高品質の製品・サービスを提供する。

76. 英国のサイバーパワーを強化し、デジタル分野の成長と輸出を促進するには、高品質で信頼性の高い企業で構成される活気あるサイバーセクターが必要である。英国企業は世界をリードする技術、トレーニング、アドバイスを、国内と世界の産業界および政府に提供している。しかし一部の企業は、最先端技術の開発に向けて、実現可能な製品の提供段階に達するための支援や投資へのコネクションが必要である。

77. 企業はまた、他社と同様に政府に承認された条件に沿ってイノベーションを進めているという確信が持てなければならない。さらに、品質にばらつきのある多種多様な製品やサービスが存在する複雑な現状において、企業の購買活動を支援する取り組みもいっそう必要であろう。それはすべて、サイバーエコシステムの需要を喚起し、さらなる成長を促すことにつながるはずである。英国は2025年までに以下のことを実現する。

78. サイバーセクターの前年比成長率が世界平均を上回ること（トレードや輸出を含めて）。英国はサイバー企業が国内外の新市場に進出することを支援する。世界的なサイバーイベントの国内開催を支援するとともに、特にイノベーション力のあるサイバー企業をトレードミッションや国際サイバーフェアに招待する。また、公共部門の調達をより効果的に活用し、NCSC認定プロバイダーの総合ディレクトリを確立して、高品質のサイバーセキュリティ製品およびサービスの需要を喚起する。

79. サイバーセクターのイノベーション力をさらに高める。これはすでに初期投資段階で大幅に増強しており、創業可能だった企業は成長と拡大を実現している。新プログラムのCyber Runway（サイバーランウェイ）は、Tech Nation Cyber Programme、Cyber101、Hut Zero等のこれまでのプログラムで得られた教訓を基に、企業支援の単一の焦点として機能している。また、サイバーアクセラレータの「NCSC for Startups」を有するチェルトナム・イノベーションセンターを、真の国際的イノベーションセンターとしての国家サイバーイノベーションセンターへと転換していく。さらに、共創を促進し支援するための既存の組織、例えば「国家安全保障技術およびイノベーションエクスチェンジ」（National Security Technology and Innovation Exchange）の専門知識を活用する。くわえて、国営英国ビジネス銀行（British Business Bank）と提携し、国家安全保障戦略投資ファンド等を通じて、初期段階にあるサイバー新興企業への高リスク投資を促進していく。

80. 英国サイバー経済の大幅な地域格差是正。サウスイースト（イングランド南東部）以外の地方で成長が実現し、新型コロナ・パンデミックからの回復に寄与するともに、地域レベルの経済活動を全体的に支援する。国家サイバー部隊の常設本部をイングランド北西部地方のサムルズベリーに設置して、テクノロジー、デジタル、防衛の各セクターの成長をロンドン以外で促進し、地域の新たなパートナーシップの構築を支援していく。また、ロンドンおよびイングランド南東部地方以外の地域のイノベーターや起業家が、製品やサービスを開発し、ビジネスを成長させ、高スキルのスタッフを採用するための支援を強化する。ここには、サイバー関連テクノロジー企業の成長支援を目的として自治体のチェルトナム・バラ・カウンシルが主導する、ゴールデンバレー（Golden Valley）キャンパスが含まれる。また、国内の多くの地域のサイバー企業の輸出能力を強化するため、地域のサイバークラスターとの連携や、サイバー産業の実力を海外のバイヤーに紹介するイベントの開催を実施していく。

81. より多くの企業が、独立的に検証される品質基準を満たすサイバーセキュリティ技術、製品、サービスを提供できるようになり、ユーザーの信頼感を高める。このことは、2021年9月にNCSCが発表した白書「NCSC技術アシュアランスの将来」に沿って実現していく。そのために、NCSCのブランドと専門知識を活用しつつ、英国の消費者が安心してサービスを購入できる信頼のおけるマーケットプレイスを構築し、セキュリティを高め、国家のサイバーセキュリティ水準を向上させていく。[23]

[23] 国家サイバーセキュリティセンター、White paper: The future of NCSC Technology Assurance（「白書：NCSC技術アシュアランスの将来」）(2021年)

Cyberfish Company CEO・創設者 ベータ・パッペンハイム

CyberFishは政府のサイバーアクセラレータープログラム参加企業です。当社のミッションは、企業と政府機関が、サイバーインシデント等で引き起こされるビジネスの混乱にうまく対処できるよう、準備を支援することです。そのために、インシデントのシミュレーション演習や、ストレス下のチームダイナミクスの観察、改善策の指導を行っています。多くのアドバイザーが得意とするのは、インシデント対応の技術的側面か、または、リーダーシップと意思決定の行動的側面のいずれかです。当社はその両方を、それぞれの専門的な知識を活用してアドバイスします。これまで、世界中のミッションクリティカルなチームで活動する500名近い業界リーダーを対象に、視点を変え、チームワークを強化し、危機対応と意思決定の改善へとつなげていく支援をしてきました。

サイバー分野での就職・転職や起業をお考えの方に

82. 従来の戦略は、英国におけるサイバー分野のスキルベースおよびサイバーセキュリティサービスセクターの成長に大きな重点を置いてきたが、戦略的背景でも説明したように、現在、**セクターと輸出の成長**において大きな成長が実現している：

サイバー企業の国際市場の開拓を支援。英国のサイバーサービスの輸出は、2020年に42億ポンドに拡大。

サイバーエクスチェンジはオンラインのサイバーポータルとして、英国全土のサイバー企業を一つにまとめている。

サイバー成長パートナーシップは、成長を阻む障壁を取り除くための、政府と産業界のパートナーシップである。

83. 過去5年間、以下のようなプログラムや企業が**イノベーション企業の成長とスケールアップを支援**し、英国のサイバーエコシステムの活発化を実現してきた：

スタートアップのためのNCSCは、イノベーターに最重要の戦略的課題を指し示すもので、すでに多くのスタートアップ企業が160以上の新しい企業トライアルに参加している。

LORCAの支援により、これれまで、72のサイバーイノベーターが2億ポンド以上の資金を集め、3700万ポンド以上の収益を上げている。

サイバーランウェイは、HutzeとCyber101の成功に基づき、イノベーターによる事業の立ち上げ、成長、規模拡大を支援している。

84. サイバー労働市場は年間1万人の専門職が不足しており、その解消のために様々な取り組みがなされてきた：[24]

サイバーファースト奨学金制度は大学学部生を支援するもので、毎年数百名に実務経験を積んでサイバー人材として活躍する道を開いている。

産業界が策定したサイバー分野の実習制度基準は、現在4種ある。また、初期学習成果を目指す3つのサイバー実習制度が、教育省の「仕事のための各種コース（Courses for Jobs）」イニシアチブを通じて提供されている。

サイバー合宿は、新設の国家技能基金（National Skills Fund）の支援のもとで9回実施されており、参加者にサイバー分野の就労機会を開いている。次の支出期間もさらに毎年実施される予定である。

85. サイバー人材の専門化により、組織は必要なスキルを明確に把握でき、個々人は理解しておくべきことを容易に調べることができる。

英国サイバーセキュリティ会議は、世界初のサイバーセキュリティ職業団体である。明確で一貫性のある職業基準の設定を開始しており、既存職業団体によるこれまでの取り組みも活用している。同会議は、現在存在する無数の資格の中から効果的な資格を明確に特定していく予定である。

サイバーセキュリティ・ボディオブナレッジ（CyBOK） は、サイバーセキュリティセクターの教育および職業訓練に情報提供し、その基盤となるものである。

[24] デジタル省、Understanding the cyber security recruitment pool（「サイバーセキュリティ分野の人材プールを理解する」）(2021年)

86. 誰もがサイバー人材として活躍できることを目指して、サイバーセクターにおける格差の是正に取り組んでいる。現状では、セクターの労働人口に占める女性の割合は16パーセントにとどまり、上級職に限って見れば女性やエスニックマイノリティの割合はわずか3パーセントである。[25]

サイバーファースト（CyberFirst）が提供する様々なコースとディスカバリープログラムは、過去5年間に、11～17歳の若者およそ30万人の参加をみた。

英国サイバークラスターコラボレーションは、産業界と学校・カレッジとの間でパートナーシップを築き、機会と専門知識があらゆる地域に行き渡るよう取り組んでいる。

国家犯罪対策庁のサイバーチョイス（Cyber Choices）は、若者が情報に基づく選択をし、サイバースキルを合法的に活用するよう支援するプログラムである。啓発活動を実施し、実習制度や就職斡旋等のより良い選択肢を提供している。

[25] 英国政府、Cyber security skillls in the UK labour market（「英国労働市場におけるサイバーセキュリティスキル」）(2021年)

第2の柱：
サイバー
レジリエンス

レジリエントで豊かなデジタル国家を構築する

87. サイバーセキュリティおよびレジリエンスは、サイバー大国としての英国の広範な戦略目標の基盤となるものである。デジタル技術の潜在的変革力を最大限に活用し、より良く、より公平で、より強靭な社会を再構築し、英国の戦略的優位をサイバー空間の内部およびサイバー空間を通じて守っていくうえで、サイバーセキュリティおよびレジリエンスは必要不可欠である。英国は、デジタルネットワーク、情報、資産を国、地域、個人の各レベルで保護し、インシデント発生時のレジリエンスを確保するための行動をとりつつ、強力なサイバー防衛を持続的に構築していかなければならない。

88. 本章ではサイバーレジリエンスに焦点を当てるが、それが十分に効果を発揮するには、英国のレジリエンスを向上させる全体的、全社会的な取り組みの一部となる必要がある。統合レビューの主要コミットメントの一つである国家レジリエンス戦略が、国家的レジリエンスへの包括的アプローチを示すものとして近日公表される予定である。

89. 英国のサイバーレジリエンスはこの10年間に大きく向上した。国家サイバーセキュリティセンター（NCSC)の設立、アドバイスやガイダンス、その他各種のツールの充実、そして、ネットワーク・情報システム規制（NIS規制）、一般データ保護規制、データ保護法2018といった法整備が実現した。しかしなお深刻な課題が残っている。政府、企業、組織、個人が様々なサイバー侵害の被害を受けており、多くの組織が引き続き多数のサイバーセキュリティ侵害や攻撃を報告している。

90. 英国は、従来の戦略の基盤の上にアプローチを進化させ、英国のサイバーレジリエンスのレベルアップを実現する。特に重点を置くのは以下の点である。

- インターネットの自動的安全性を高める取り組みを拡大する。攻撃を防ぎ、すべての英国企業、組織、国民のための基本的保護を構築し、オンラインでの自衛が難しい人々へのサポートを拡大する。
- 政府がサイバーセキュリティのベストプラクティスの模範として行動するための野心的目標を設定する。
- サイバーセキュリティを優れたビジネスの中核要素として定着させる。規制やその他のインセンティブを有効利用し、脅威への洞察力を活用して、自衛能力のあるコミュニティを構築する。
- これらすべてのことを、客観的に測定可能な基準、証拠、データによって裏打ちし、単なるデータ収集で終わることなくデータに基づき実際に行動する。

91. 本戦略におけるサイバーレジリエンスの概念には3つの重要な側面がある。第一に、**リスク**の本質を理解する必要がある。第二に、サイバー攻撃を防止し、これに抵抗するために、システムの**セキュリティ**を強める対策を取る必要がある。第三に、それでも攻撃は起こりうることを認識して備えを固め、影響を最小限に抑えて回復するのに十分な**レジリエンス**を高める必要がある。

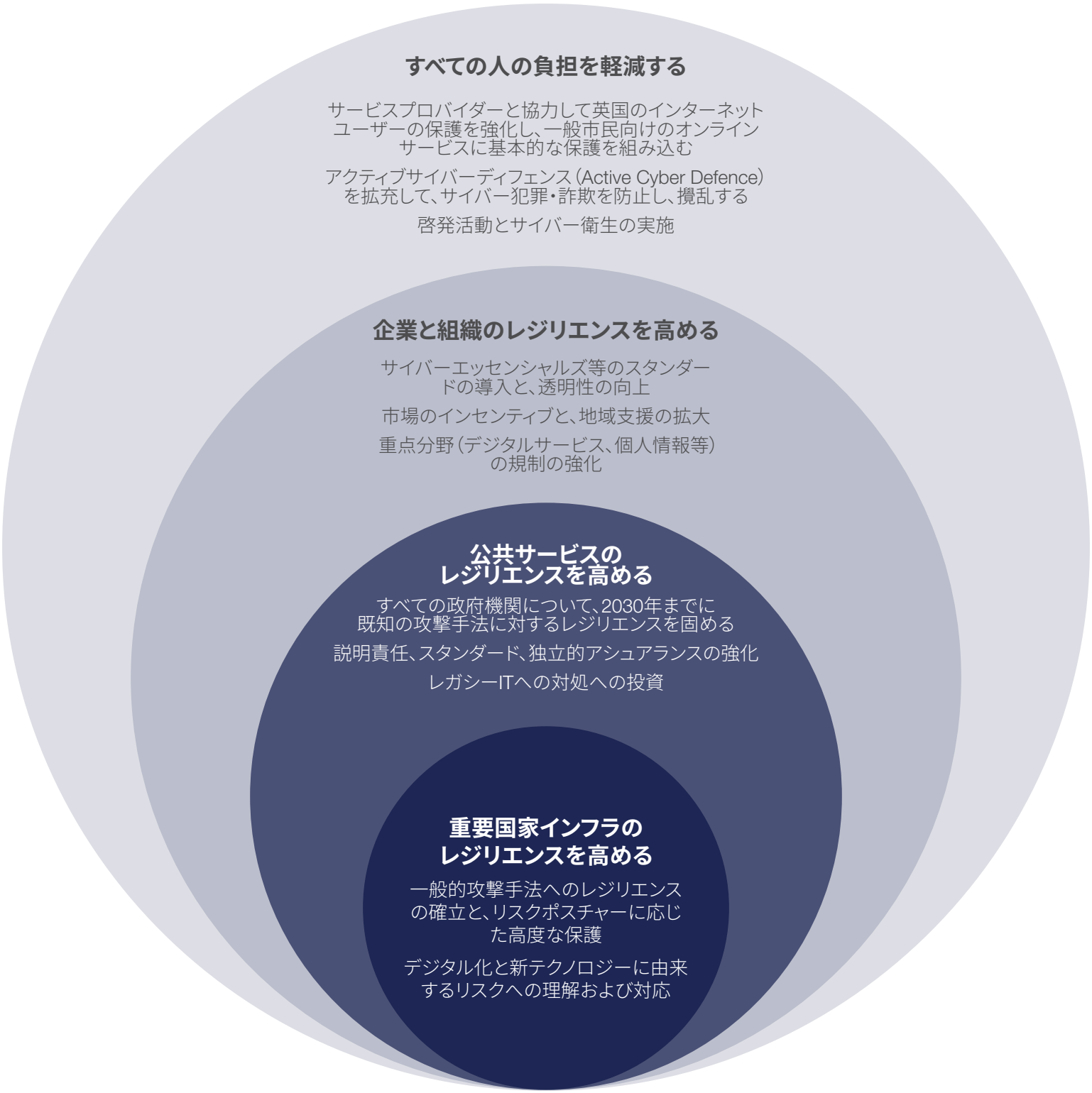
92. 取るべきアプローチはそれぞれの対象に合わせて異なるものとなり、全システム的なリスクに対処する様々な国家的能力がこれを支えていく。ここで保護と影響を与える対象とは、英国国民、企業・組織、政府・公共部門、そして重要国家インフラの運営者（すなわち、飲料水、電気、金融、運輸、通信といった、すべての人が依存する主要サービスの提供者）を指す。

93. 最初の重要ステップとして、英国の全インターネットユーザーのデジタル環境を保護し、攻撃を防ぎ、製品とサービスに基本的セキュリティを組み込むとともに、個人と中小企業・組織に対してサイバーセキュリティ改善のための基本的対策を取る支援を行う。そのうえで、より大きな責任と能力を持つ者がリスクに見合った追加的セキュリティとレジリエンスを導入するようになれば、国民と経済を支える重要公共サービスや基幹サービスに必要な最高水準の保護が実現するだろう。

94. この努力は、政府と全経済・社会が共有して行う取り組みでなければならない。企業や組織の役員は、自らのサイバーリスクを管理する責任を負う。目的は、インセンティブや、支援、規制からなる適切な枠組みに支えられた明確な期待を設定して、改善を実現し、サイバーセキュリティリスクの負担をエンドユーザから適切な立場にいる管理者に移していくことにある。

95. 政府省庁、広範な公共部門、重要国家インフラ（CNI）の規制対象事業者に対しては、基準を引き上げて、より積極的なリスク管理の実施を義務付けていく。デジタルサービスおよびプラットフォームのプロバイダーを含む大企業・組織に対しては、事業運営の中核として、自社システム、サービス、顧客の保護に説明責任を果たすことを求めていく。そして見返りとして、政府はデジタル環境の保護とシステムリスクへの取り組みを強化するとともに、アドバイス、ツール、市場での認定、改善に役立つスキルの開発を通じて支援を提供していく。

96. 英国のサイバーレジリエンスの推進は、国際的取り組みの一環として行っていく必要がある。サプライチェーン、ITプラットフォーム、多国籍企業、そしてインターネットそのもののグローバル化が進展するなかで、英国が単独でサイバーセキュリティを向上させることは不可能である。この課題への対応として、英国は引き続き、英国と世界のサイバーレジリエンスのつながりについて理解を深め、高リスク分野に対処し、パートナー諸国との協力のもとでレジリエンスを構築して、デジタル変革、安全保障、そして通商を促進していく必要がある。これは相互利益に資するものであり、詳しくは第4の柱：グローバルリーダーシップの章で説明する。


すべての人の負担を軽減する
サービスプロバイダーと協力して英国のインターネットユーザーの保護を強化し、一般市民向けのオンラインサービスに基本的な保護を組み込む
アクティブサイバーディフェンス（Active Cyber Defence）を拡充して、サイバー犯罪・詐欺を防止し、攪乱する
啓発活動とサイバー衛生の実施
企業と組織のレジリエンスを高める
サイバーエッセンシャルズ等のスタンダードの導入と、透明性の向上
市場のインセンティブと、地域支援の拡大
重点分野（デジタルサービス、個人情報等）の規制の強化
公共サービスのレジリエンスを高める
すべての政府機関について、2030年までに既知の攻撃手法に対するレジリエンスを固める
説明責任、スタンダード、独立的アシュアランスの強化
レガシーITへの対処への投資
重要国家インフラのレジリエンスを高める
一般的攻撃手法へのレジリエンスの確立と、リスクポスチャーに応じた高度な保護
デジタル化と新テクノロジーに由来するリスクへの理解および対応

目的1：サイバーリスクへの理解を深め、サイバーセキュリティおよびとレジリエンスに関する効果的な行動を促進する。

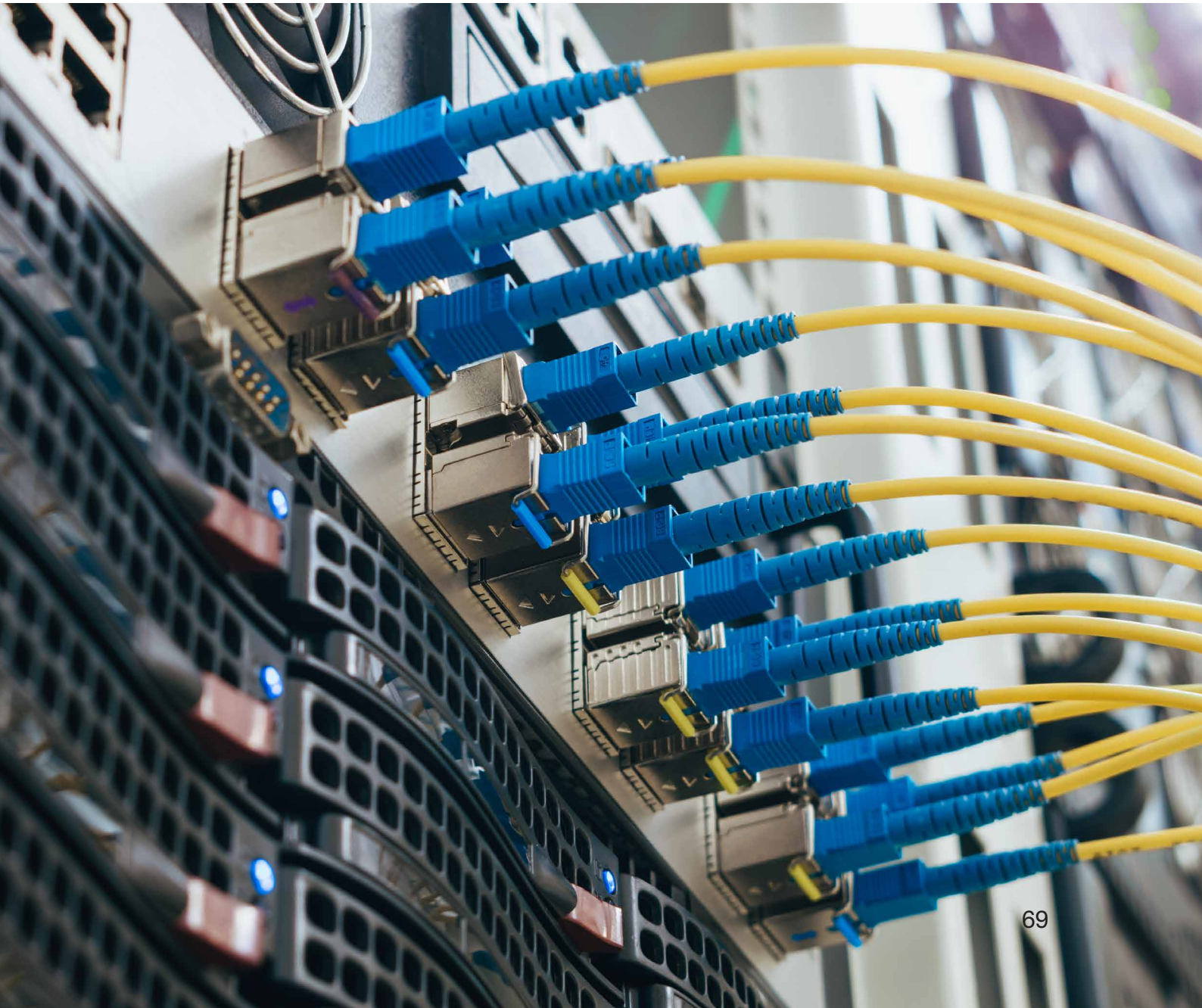
97. 英国は、政府、企業、組織の間のパートナーシップをいっそう緊密化し、リスクに対する理解を集合的に深め、優先課題を定めて、行動に移すための根拠を確立していく。消費者にサービスを提供する企業や組織との協力を通じて国民を支援するとともに、分野横断的なリスクを特定する政府の能力をいっそう強化していく。英国は2025年までに以下のことを実現する。

98. 政府が国家のサイバーリスクについて最新の戦略的理解を有している。そしてこの理解に基づいて、全システム的リスクを特定し、優先課題を伝え、戦略と実施を推進する。英国は、先の国家サイバーセキュリティ戦略に基づく「脅威の理解」への多額の投資を今後も維持し、そこからさらに価値を引き出していく。また、相互接続が進む世界におけるリスク理解のための既存の取り組みも活用していく。ここには、デジタルサプライチェーンが過度に集中している分野の特定や、パートナー諸国と協力して集団的リスクを管理することが含まれる。また、コンピュータ不正利用法（CMA）違反の記録の改善、データ侵害と下流犯罪の関連性の理解、CMA違反が他の種類の犯罪行為をどのように助長しているかに関する知識の拡充も行う。

99. 政府がサイバーリスクに対する理解において模範となる。NCSCのサイバー評価フレームワーク（CAF）を全政府機関のアシュアランスフレームワークとして採用し、重要システムと共通サプライヤーのマッピングを行う。新たに政府サイバー調整センター（GCCC）と政府横断的な脆弱性報告サービス（VRS）を設立し、政府がインシデント、脆弱性、脅威の管理にあたって「一体として防衛する」ことを可能にする。VRSは、セキュリティ分野の研究者コミュニティと価値ある信頼関係を築き、政府機関全体の脆弱性削減を実現することを目指す。また国内自治政府の同様の取り組みへの支援、およびそれとの調整も継続していく。例えば、現在提案されているスコットランドのサイバーレジリエンスのための中央調整機能の設置がこれにあたる。

100. 英国の重要国家インフラ全体を通じて、サイバーリスクに対するより精密な理解を確立する。英国は、サイバー評価フレームワーク（CAF）またはそれと同等のものを重要国家インフラセクター全体で採用し、現在使用されている他のサイバーセキュリティ評価・報告フレームワークとの比較可能性を改善していく。また、重要国家インフラとそのサプライチェーンにおけるクリティカリティレビューと依存関係のマッピングを完成させる。そして、脅威およびリスク情報へのアクセスを改善するために、重要国家インフラの所有者・運営者との連携を密にし、リスクポスチャーについて合意する。さらに、デジタル化や新技術の結果として新種のリスクや新たな重要国家インフラが出現している場所の理解に努める。ここには、ネットゼロへの移行等、より広範な優先課題の一環としての取り組みも含まれる。

101. 英国企業・組織が、サイバーリスクとその管理責任についてより良く理解している。英国は、組織が顧客に対するリスクについてよりよく理解できるよう支援する。例えば、組織の保有するデータが詐欺や個人情報の盗難、恐喝などの犯罪にどう利用されうるか、といった問題である。また、サイバー攻撃の普及と影響や、各セクターのサイバーセキュリティ改善に関する相対的進展状況についての調査とデータから得られる知見を、これまでよりもいっそう共有していく。



目的2：サイバー攻撃をより効果的に防止しこれに抵抗するために、英国の組織内のサイバーリスク管理を改善し、国民の保護を強化する。

102. サイバー攻撃を防止し、それに抵抗するための英国のアプローチは、以下のことを前提としている。(i) 組織は自らのサイバーリスクを管理するために行動を起こす責任がある。しかしこれを優先課題とするには、取締役会レベルの説明責任および優れたガバナンスの強力な枠組みが必要である。(ii) 政府は、それが可能な場合には、大規模かつ直接的にリスクを削減するための措置を産業界と協力してとっていく役割がある。(iii) 個人、個人事業主、小規模企業・組織に対しては、サイバーリスクを管理できるよう支援と指針を確実に提供しなければならない。英国は2025年までに以下のことを実現する。

103. 政府が英国への危害を大規模に削減し、英国国民の負担を軽減している。 政府は、英国のすべてのインターネットユーザーのために、問題の上流での対処を増やしていく。アクティブサイバーディフェンスの施策を拡大して、チャリティ団体、学術機関、中小企業、一般市民を含む幅広いセクターを支援していく。また、各種オンラインサービスの保護も産業界との連携や情報共有を増やすことを通じて強化していく。

104. こうした取り組みは、英国国民のオンライン保護を目的とした政府の他の優先課題、例えばオンライン安全法案の作成や詐欺等の経済犯罪対策等を補完するものである。

105. このことは、関連セクター（例えばオンラインサービスプロバイダー、電気通信、テクノロジー、銀行、小売等）とのより緊密な協力を通じて、英国のインターネットユーザーの保護を強化していくことを意味する。違法目的のウェブサイト登録をより困難にすることや、オンラインの悪質コンテンツの削除・ブロックを増やすこと、盗まれた認証情報の回復と返却の改善、英国の電気通信インフラのセキュリティ強化等がその方策である。また、自主的な取り決めが不十分だと判明した場合には、国民の保護に法的裏付けを与えるオプションも用意していく。

106. 大規模被害を減らすための英国の取り組みには、デジタルサプライチェーンに由来する全システム的なリスクへの対策も含まれる。英国政府は、電気通信分野で行っているように、必要に応じてサプライチェーンの多様化促進のために介入する。集団的経済安全保障を強化するために情報共有を改善し、重要セクターにおける外国直接投資（FDI）の審査に堅牢かつ予測可能で適切なアプローチを採用し、政府の重要かつ共通サプライヤーについて明確な要件を確立する。

107. 2030年までに、政府の死活的に重要な機能がサイバー攻撃に対して大幅に強化され、あらゆる政府機関が（公共部門全体を通じて）既知の脆弱性と攻撃手法に対するレジリエンスを獲得している。 英国は、公共部門をベストプラクティスの模範にすることを目指す。これを実現するために、初の政府サイバーセキュリティ戦略を発表する予定である。これが重点を置くのは、効果的なリスク管理のプロセス、ガバナンス、アカウンタビリティ、中央集権的な各種能力（アクティブサイバーディフェンス等）、システム、ネットワーク、サービスの包括的なモニタリング、迅速かつ大規模なインシデント対応、スキル、知識、文化への投資を通じた持続的な変革の推進である。

108. 英国の重要国家インフラへのサイバーリスクが、より効果的に管理されている。重要国家インフラは言うまでもなく、国が最も依拠するサービスである。英国は今後も引き続き事業者と密接に協力して、一般的攻撃手法へのレジリエンスをできるだけ早急に達成するとともに、必要に応じてより高度な保護を導入していく。このことは、NIS規制で指定する基幹サービス運営者にとっては、各セクター所轄官庁が設定する基準を少なくとも満たさなければならないことを意味する。

109. このような成果を実現するには、重要国家インフラ事業者が重要システムのサイバーセキュリティに投資し、サプライチェーンを含むリスクを効果的に管理するようにしなければならず、そのために政府が事業者責任を追及する権限について見直しを行う。英国政府は、広範な国家安全保障上のリスクと急速に変化する脅威や技術を考慮に入れつつ、規制の枠組みを強化し、その適用範囲、権限、適応のための機敏性を向上させていく。手始めに、NIS規制の改革に関する協議を実施し、英国の電気通信事業者に対する新しいセキュリティの枠組みを実施する。また、適切な規制枠組みを新たに策定し、ネットゼロの実現に必要なスマートで柔軟な将来型エネルギーシステムがサイバー脅威に対して安全かつレジリエントであるようにしていく。

110. 上記と並行して、規制当局の能力強化、技能への投資を通じ重要国家インフラ事業者がサイバー専門職を採用、育成、保持できるようにすること（「英国のサイバーエコシステム」の章を参照）、重要サプライヤーとの連携強化による事業者サプライチェーンのリスク管理支援（ガイダンス、立法、調達関連提案等）を行う。

111. データ利用の基盤となるインフラが安全でレジリエントである。このインフラは死活的に重要な国家資産であり、経済を支え、公共サービスを提供し、成長を促進する。英国政府は、データが処理、転送、または外部のデータセンター等で大規模に保存される際に適切に保護されるよう、これまで以上に大きな役割を果たしていく。セクター全体でより高いセキュリティおよびレジリエンス基準が維持されるよう、強力なリスク管理の枠組みを構築するとともに、国家安全保障・投資法 2021の規定を実施して投資審査を強化する。パートナー諸国との連携を強化つつ、グローバルなデータアクセスとフローの増加が英国のセキュリティリスクの増加につながらないようにし、大量のデータ収集で生じるセキュリティ課題にも対処していく。

112. また、英国データインフラサービスの経済的基盤としての枢要性の増加、および、重要国家インフラにおけるその役割についても検討する。これらの措置は、国家データ戦略および統合レビューで定めたコミットメントに従ったものである。

113. より多くの英国の企業と組織が、サイバーリスクを積極的に管理し、サイバーレジリエンス向上のための行動をとっている。英国は、効果的なサイバーセキュリティを奨励する市場インセンティブの開発を通じて、支援を提供し行動変革を促していく。またこれを補完するために、必要に応じて的を絞った法律を制定し、サイバーリスクが最高責任者によって効果的に管理され、英国のサイバーセキュリティ法がリスクや技術の絶えざる変化に常に適合するようにしていく。

114. このような目的を達成するために、政府は、市場で影響力をもつ調達者、金融機関、投資家、監査人、保険会社との協力を進め、経済全体で優れたサイバーセキュリティの実践を奨励していく。特に、リスクへのレジリエンスに関する企業報告の改善案として、サイバーリスクへのレジリエンスも含むよう提案する。これにより、投資家と株主は、企業が自社事業のマテリアルなリスクをどのように管理し軽減しているかについて、良く理解することが可能になる。また、サイバーエッセンシャルズ認証スキーム等の認定や基準の取得を引き続き促進するとともに、企業のサイバーリスク管理における取締役会レベルの関与を促していく。

115. サイバー攻撃の潜在的影響が最も大きいセクター、例えば、特定の基幹サービスやデジタルサービスのプロバイダー、経済全体のデータ保護、大企業等に的を絞った法律を制定していく。またこれを補完するものとして「デジタル規制のための計画」を策定する。まず、上記および「技術的優位」の章で説明するように、ネットワーク・情報システム（NIS）のセキュリティを管理する規制に重点を置き、次に、英国の個人データ保護体制の改革へと対策を進めていく。

116. 英国の企業と組織全体のビジネスレジリエンスおよびサイバーセキュリティの向上のための取り組みは、「サイバーセキュリティ規制およびインセンティブのレビュー」で詳しく説明される。

117. サイバーレジリエンスを向上させるための技術的アドバイスや、自助的なツール、保証された製品・サービスが容易に利用できるとともに、特に一般市民、個人事業主、小規模組織の支援を重視しつつ持続的に改善されていること。
英国は、NCSCを通じて、技術的に正確で、タイムリーで、実用的なガイダンスや自助的ツールの開発を継続していく。一貫性があり明確なメッセージを、最も効果的なチャネルを通じて提供していく。それは例えば、サイバーアウェアキャンペーンや、NCSCのウェブサイト、政府、法執行機関のネットワーク、産業界とのパートナーシップ等である。また、地域レベルで利用できる支援も充実させる。関心をもつ成人を対象とした「必須デジタルスキル」資格制度には、「デジタル資格授与」(Digital Entitlement) を通じて今後も引き続き十分な資金を提供していく。これにより学習者は、オンラインで安全かつ責任ある行動をとるための基本的デジタルスキルを習得できる。さらに、企業と組織が複雑なサイバーセキュリティ市場を活用していくための支援として、保証製品・サービスのための枠組みを拡張するとともに、サイバーエッセンシャルズに関する商業サービスを開発して中小企業が基本的アドバイスを容易に利用できるようにしていく。

タリアン (Tarian) 地域サイバー犯罪対策ユニット・サイバー保護・防止担当官　エリス・パワー

タリアン地域サイバー犯罪対策ユニットは、ウェールズ警察から出向している警察官と職員で構成される分野横断的なチームである。ウェールズ南部で、より安全かつ堅牢なサイバー環境を提供することを使命としている。

サイバー保護・防止担当官、エリス・パワーはエンゲージメントチームで職務を遂行している。

「月並みな表現ですが、当ユニットに典型的な一日というのはありません。日によっては、警察内部や外部の組織に対して、サイバーの脅威から自分と職場を守る方法について確実に理解してもらうよう、アドバイス等のプレゼンテーションを行うこともあります。また、学校の生徒たちに、インターネットの安全性や1990年コンピューター不正利用防止法などの様々なトピックについて話をすることもあります。連携機関や部隊との会合にも頻繁に出席し、新種の脅威や対象者向けの関連ガイダンスについて議論しています。さらに、脆弱性の警告を受けた組織と関わったり、国家的作戦に参加したり、関連イベントや会議にゲスト参加したり、あるいは時間を見つけて自分自身の能力と知識ベースの継続的な向上を図っています。」

目的3：
サイバー攻撃に備え、対応し、そこから回復するために、国と組織レベルでレジリエンスを強化する。

118. リスクの理解や予防策の実施という取り組みを行っても、一定のインシデントは依然として発生するだろう。被害を最小限に抑え、被害者の支援を強化するには、インシデントの管理と対応の能力をあらゆる組織で強化する必要がある。英国は2025年までに以下のことを実現する。

119. 国家的に重大なサイバーインシデントへの対応に関する英国の戦略的管理および調整が、いっそう効果を高めている。英国は、重大サイバーインシデントへの対応に関する政府のこれまでの経験に基づき、政策とプロセスの改善にあたって特定の教訓が活用されるようにする。危機管理の経験をパートナー諸国や産業界と共有する一方、他国のベストプラクティスを特定して、英国自身の準備とプロセスを強化していく。また、NCSCおよび法執行機関のインシデント管理チームが、絶えず進化するインシデントのあらゆる種類に対応できるよう必要な専門知識と手段を整えるとともに、優先的脅威への国家対応を調整していく。

120. サイバーインシデントの報告が容易で、サイバー犯罪の被害者はより良いサポートを受けることができる。報告された情報は将来の事件防止にも役立ち、サイバー犯罪者を捜査し、その行為を破壊し、起訴するための法執行機関の支えとなる。そのために、アクションフロード（Action Fraud）に代わる新たな国家的詐欺およびサイバー犯罪報告・分析サービスを、2025年までに実現する予定である。また、これ以外の方法によるサイバーインシデント報告も奨励していく。例えばロンドン市警察の新しい企業報告機能もその一つである。規制対象セクターに対しては、規制当局が「ニアミス」を含む広範なインシデントの報告を義務付けられるようにする。さらに国家経済犯罪被害者ケアユニットを展開し、ストレスの大きい有害な経験をした被害者へのサポートとガイダンスを改善する。

121. 政府と重要国家インフラが、インシデント対策の改善と定期的演習等を通じて、インシデントに対応しそこから復旧するための体制を整えている。今後、英国政府と重要国家インフラ事業者が必要なサイバー演習およびインシデント管理サービスを市場で調達できるよう、サイバーインシデント対応に関するNCSC認定スキームを拡大し、演習に関する新たなスキームも導入していく。

122. 政府内部では、部局内および政府のデジタル資産全体にわたって監視と検知の機能を改善していく。また、教訓を特定して政策とプロセスの改善に活用していく。例えば、危機管理の経験をパートナー諸国および業界と共有し、英国内のインシデント管理チームが、絶えず進化するインシデントのあらゆる種類に対応するのに必要な専門知識、能力、機能を有するようにする。

123. 重要国家インフラにおいては、事業者全体の演習、試験、敵対者シミュレーションに関する明確な要件を定めるとともに、インシデント対応および演習におけるイノベーションとコラボレーションを、金融セクターサイバーコラボレーションセンターのようなモデルの適用も検討しつつ奨励していく。また、技術に関する英国の野心的目標（次章で説明）の一環として運用技術セキュリティの国立研究所を設立し、産業界、学術界、パートナー諸国と協力しつつ、同分野の能力構築のため重要産業技術の試験、演習、訓練の中核拠点としていく。

124. 英国の企業と組織が、インシデント発生時に何をすべきか、誰に連絡すべきか、誰の支援を得て、どのように復旧するかについて、明確に理解している。
英国は、保証された業界サービスの支援を受けつつ、訓練と演習へのアクセスを改善していく。例えば、新しいサイバーインシデント対応スキームやサイバーインシデント演習サービスがこれにあたる。また、サイバー犯罪の被害者個人が全国規模の一貫した法執行支援を受けられるようにするとともに、中小企業・組織に対しては、地域サイバーレジリエンスセンター等の地域支援を活用するよう働きかけていく。

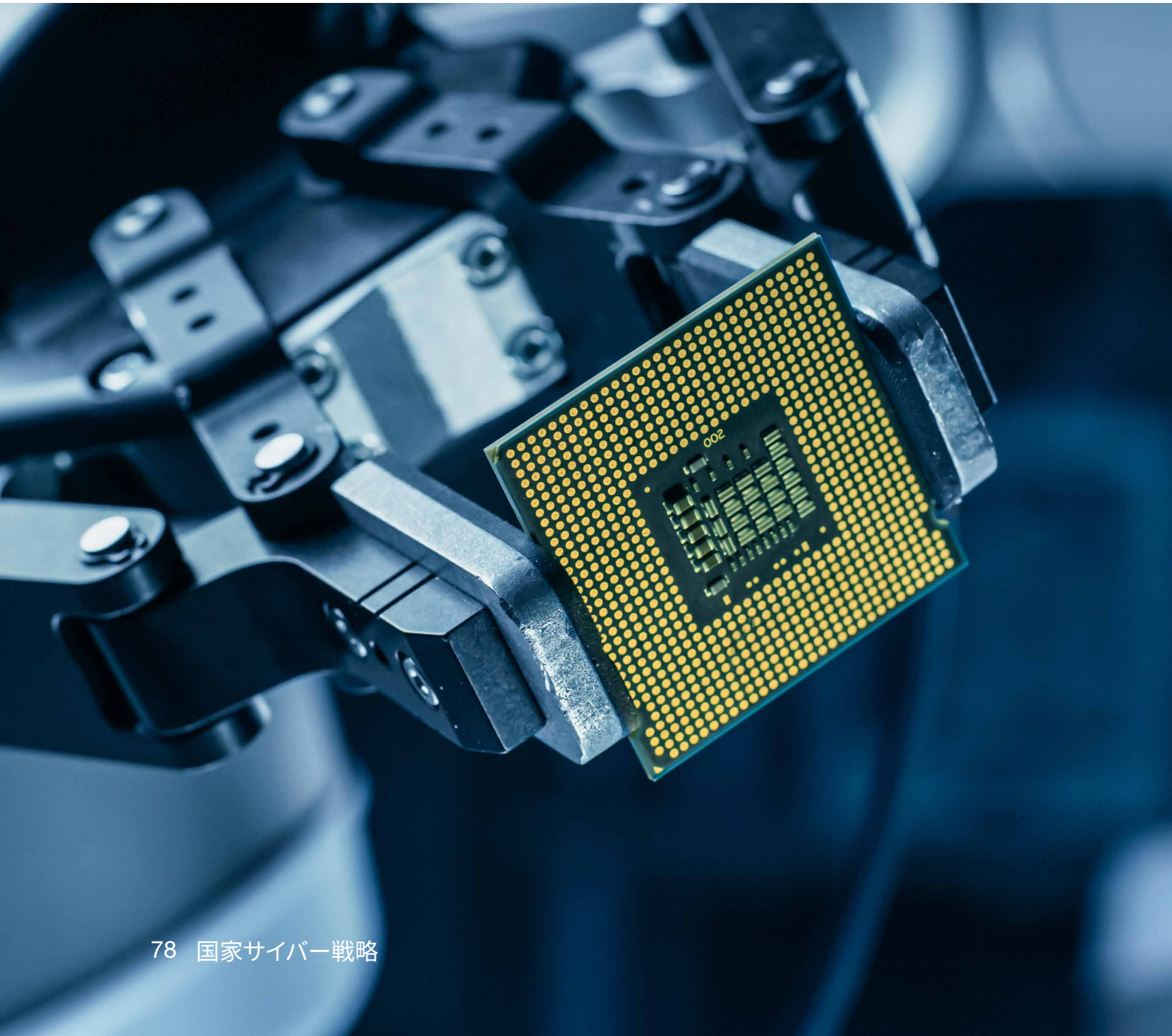
CyberOwl CEO　ダニエル・ング

CyberOwl社は、政府のサイバー開発プログラムの恩恵を受けています。当社は海運および重要国家セキュリティ両セクターにおける運用資産のサイバーセキュリティ監視および分析を行っています。サステナビリティの推進で現場資産の接続性とデジタル化への需要が高まるなか、サイバーリスクも増大しています。当社では、事業者が資産を特定してマッピングを行い、サイバーリスクの早期の警告を手にし、安全確保を自社自身と規制当局に証明する支援を行います。EMEA（欧州・中東・アフリカ）およびアジア太平洋全域にわたって世界有数の海上資産運用会社と協力し、世界の海運物流サプライチェーンのレジリエンスの向上を実現しています。2021年は契約件数が14倍に増え、英国とシンガポールでの事業を倍増させました。

Rapid7 コミュニティ&パブリックアフェアーズ担当バイスプレジデント　ジェン・エリス

私の業務は、あらゆる規模・業種の組織のセキュリティ専門職やリーダーと相談しつつ、現実的課題を理解し、サイバーセキュリティを高めるソリューションを見つけることです。組織の多くが問題に圧倒され、重点分野や、どこから手を付ければいいのか、どうすれば改善するのかが分からなくなっていると聞きます。また、技術担当者が上層部の同意を得にくいというケースもあります。政府による明確で一貫した透明性の高いサイバー戦略があれば、このような問題に対処できるはずです。技術担当者が上層部を説得する材料になるうえ、注力すべき重点分野や、成熟への潜在的な道筋も明らかになるからです。サイバーセキュリティは依然としてきわめて複雑で、終わりがありません。しかしサイバー戦略の普及により、その重要性への理解は深まっており、一致団結して取り組んでいるという実感も生まれています。

第3の柱：
技術的優位



サイバーパワーに死活的重要性をもつ技術を先導

125. 一部の技術は、サイバー空間の将来を形成していくうえで必要不可欠なものとなろう。そのような技術で主導的役割を確立できれば、当該技術の設計と配備の方法に影響力を行使でき、自国の安全保障と経済的優位を守り、サイバー能力の飛躍的向上の機会をより迅速に活用することが可能になる。テクノロジーは地政学的パワーの手段として重要性が高まっており、それとともにこの分野の競争も激化していくだろう。

126. 英国にとっては、科学技術、およびそれがよって立つデータへのアクセスを通じて戦略的優位を追求していくことが、サイバー大国としての広範な目標を達成するための前提条件となる。政府はこれまでの戦略では、新興企業向け振興プログラムやサイバーセキュリティ研究分野の卓越研究センター等を通じて、サイバーセキュリティ技術の研究とイノベーションを刺激し、「セキュアバイデザイン」の消費者向け機器開発を奨励する措置をとってきた。しかし現在は、重要技術への関与を維持し、競合国や敵対国への過度の依存を回避するために、より野心的かつ積極的なアプローチが必要である。

127. 統合レビューでは、英国を科学技術大国とし、科学技術を利用して戦略的優位を構築・維持するための計画を示した。本戦略は国家科学技術評議会および科学技術戦略局の活動の支援を通じてその目標を追求するとともに、人工知能、量子技術、データ等の分野における英国の戦略を補完する。

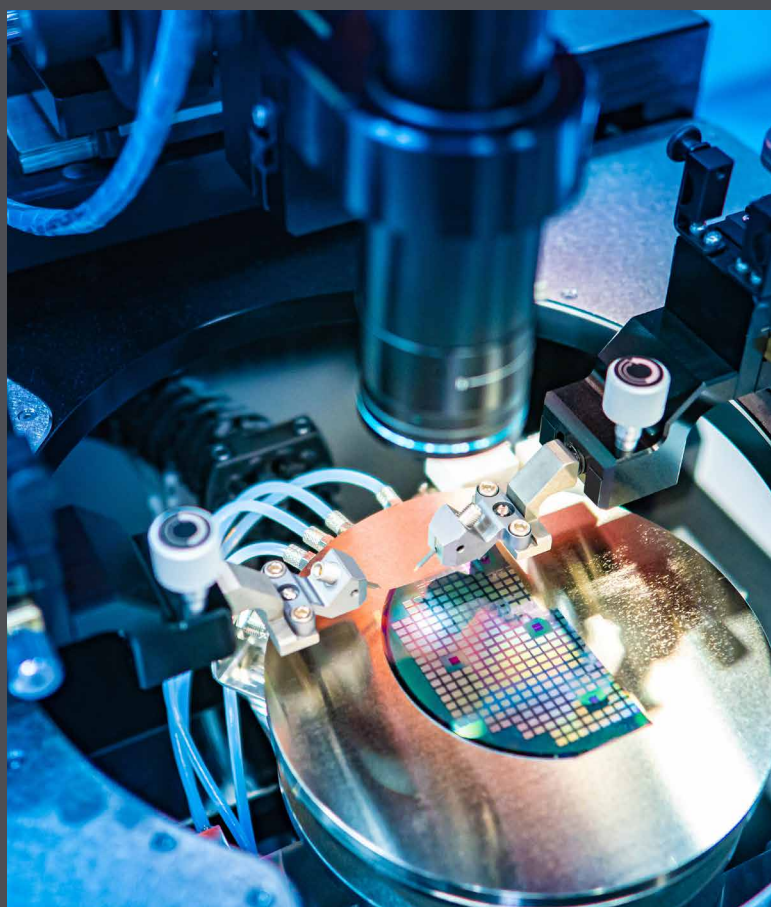
128. 英国は、国家サイバーセキュリティセンター（NCSC）と他の政府機関全体の技術的専門知識の主導のもと、サイバーパワーにとって最も重要な技術分野を特定する能力を強化していく。優先課題についての国家レベルの戦略的決定は、統合レビューで示した「所有-協働-アクセス」（Own-Collaborate-Access）の枠組みを利用しつつ行う。特定の分野では、英国の国内の能力開発に必要な研究開発活動や戦略的パートナーシップに投資していく。また、グローバル市場に依存する分野では、産業界、規制当局、パートナー諸国と協力しつつ、信頼できる多様なサプライチェーンを促進し、技術の安全性とオープン性を確保する基準の形成に取り組む。さらに新興テクノロジーによって生成されると同時にそのイノベーションを推進していく膨大な量のデータおよび情報を活用し、保護する英国の能力を、国家データ戦略で示した経済社会の便益最大化のための枠組みに則って強化していく。

サイバーパワーにとって死活的重要性をもつテクノロジー

英国のサイバーパワーにとってはさまざまな既存のテクノロジーと新興テクノロジーがきわめて重要であり、これらの発展を予測し、評価し、行動する能力が求められている。戦略の遂行にあたっては、様々な技術やアプリケーションを優先的に扱う。それは例えば以下のようなものである。なおこのリストは網羅的でも固定的でもない。英国の優先課題は、産業界、学術界、技術専門家からの意見を採り入れつつ継続的に変化していく。

- 5Gおよび6Gテクノロジー、およびその他の新しいデータ通信形態。
- 人工知能（AI）。ここには、AIシステムのセキュリティ確保のニーズや、ネットワーク監視等の幅広いアプリケーションにおけるサイバーセキュリティ強化のためのAIの活用の可能性が含まれる。
- ブロックチェーン技術とその応用。例えば暗号通貨やDeFi（分散型金融）等。
- 半導体、マイクロプロセッサチップ、マイクロプロセッサアーキテクチャ、およびそれらのサプライチェーン、設計、製造プロセス。
- 暗号認証。ID・アクセス管理や高信頼性暗号製品等。
- モノのインターネットおよび、消費者、企業、産業、コネクテッドプレイス等の物理的環境で使用される様々な技術。
- 量子技術。量子コンピューティング、量子センシング、ポスト量子暗号等。

この取り組みは、政府全体を通じた多数の戦略や成果（例えば、国家データ戦略、国家AI戦略、統合レビュー、およびこの柱における技術重視の成果等）を支援し、それに沿って行われるものである。



目的1：
サイバーパワーにとって死活的重要性をもつ科学技術の発展を予測、評価し、それに基づいて行動する能力を高める。

129. サイバー関連技術で競争力をつけ、維持していくには、科学技術の重要分野を特定・分析し、国家的取り組みとして優先していくために調整された、厳密かつ一貫性のあるアプローチが必要である。そのためには、政府と学術界の研究・技術専門知識をこれまで以上に開発していかなければならない。このことは、科学技術分野のホライズンスキャニングと情報収集のための新たな統治構造と統合される予定である。それと同時に、パートナー諸国や競合国の優先課題およびシステムの理解のために、産業界の専門家の意見を活用し、英国の海外ネットワークも活用していく。英国は2025年までに以下のことを実現する。

130. 政府が新興および開発途上の科学技術を分析する能力をもち、それが英国のサイバー政策および戦略に対して持つ意味合いを理解している。英国は、NCSCのマンチェスターの新応用研究ハブを始めとして研究能力を拡大し、政府科学局等の専門家と協力しつつ、コネクテッドプレイスや運輸等の分野における新興技術に焦点を当てていく。また、政府外の専門知識も活用する。4つのサイバーセキュリティ研究所と19のサイバーセキュリティ卓越研究センター（ACE）を支援するとともに、優先的テーマを扱う研究者に対してパスファインダー賞を授与し、英国の海外拠点および国際パートナーシップをより効果的に活用していく。

131. このような理解の向上によって、政府の広範なホライズンスキャニング、優先順位付け、意思決定への情報提供がより迅速になり、かつ効果的に行われるようになる。そしてこのために、機会の活用とリスクの軽減に対してより積極的なアプローチが可能になる。英国は、科学技術の進歩とそのサイバーへの影響を予測するために、内部的なホライズンスキャンニング機能を新設する。また、より多くの情報に基づいて重要サイバー技術を優先する決定を行い、英国の安全保障に利する研究開発および政策策定を方向付けていく。そして、必要に応じて、科学技術の優先課題に関する広範な意思決定に情報を提供する。これは科学技術戦略局や国家科学技術評議会を通じて行われる。

セキュア情報技術センター（CSIT）主席研究員、マイエ・オニール

CSITは、サイバーセキュリティに特化した英国最大規模の大学技術研究センターです。マイエ・オニール教授が主任研究員を務め、2009年に英国初のイノベーション&ナレッジセンターの一つに選定されました。CSITは、研究、イノベーション、産業界との連携に成果を上げ、過去10年間に国内外の評価を大きく高めました。北アイルランド・サイバーセキュリティクラスターの成功にとって重要な要素であるCSITは、スピンアウト活動、地域事業の規模拡大、地域内への外国直接投資を支援しています。2009年のスタート以来、北アイルランドのサイバーセキュリティセクターは大きく成長し、現在104社で2,300人を雇用。給与総額は年1億1000万ポンドに上ります。

目的2：サイバー空間に必要不可欠な技術の安全保障に関して、主権国家および他国の同盟国としての優位を育成し維持する。

132. 英国がサイバー技術の主要分野で主導的地位を確立または競争優位を確保できる潜在力を有する、または、非同盟国内の供給源への依存が許容しがたいセキュリティリスクを呈しているといったケースにおいては、国内の産業基盤の開発を追求する。分野によって、真に主権的能力を維持する必要があるものと、パートナー諸国との協力や市場の一側面でのみ主導的地位を追求すべきものもある。そのために、産学連携でイノベーションおよび研究開発を活性化させる協調的アプローチが必要である。英国は2025年までに以下のことを実現する。

133. 英国がこれまでよりも効果的にサイバーパワーの最重要技術分野において研究をイノベーションにつなげ、新興企業を支援している。英国政府は、全国の研究者が産業界のパートナーと協力して課題ベースのアプローチを採用し、研究成果を商業化・実用化していくことを支援する。これにより、最も可能性のあるアイデアを特定し、資金提供者からの投資を喚起することができる。また、イノベーション戦略で示したアプローチに基づいて、主要技術の周辺でエコシステムを確立することを支援するとともに、英国の優位をより強固かつ模倣されにくいものにしていく。

134. 英国がマイクロプロセッサの安全設計における世界的リーダーとして、いっそう強固な地位を確立。[26]英国は「デジタル・セキュリティバイデザイン」プログラムを基盤として活用ししていく。同プログラムは、ソフトウェアを脆弱性から保護するコンピュータチップのより安全な新技術の開発を実現した。この経験を人工知能プロセッサに活かし、英国のベンダーに国際市場での優位を与えていく。また、国家量子技術プログラムと協力して量子コンピュータのセキュリティモデルを設計し、英国企業が同技術で世界をリードできるようにしていく。

135. 運用技術や重要産業用制御システムのセキュリティに関する研究分野、および、それらを国内で試験・演習する能力において、英国が世界のリーダーとして評価される。英国は、産業界・学術界と連携して、運用技術セキュリティの国立研究所を設立する。ここでは世界をリードする研究プログラムを主催し、国内で当該セキュリティ技術を演習・試験できる施設を、政府、軍、産業界、そしてパートナー諸国に提供していく。また「5G通信サプライチェーン多様化戦略」で確認したとおり、英国テレコムラボ(UK Telecoms Lab)を設立し、政府・規制当局と産業界を結集して新しい通信セキュリティの枠組みを支援するとともに、英国サプライチェーンにおける通信機器ベンダーの多様性を高めていく。[27]

136. 政府が、重要サイバー技術分野における英国のイノベーションと知的財産を敵対的活動から保護し、競争力を維持できるようになる。[28]英国は、これらのテクノロジーのセキュリティ分野での技術的指導力を、その発展に合わせて提供していくのに必要なリソースおよび専門知識に投資していく。例えば、対英直接投資のリスクへについて、国家安全保障・投資法2021の目標に沿った助言を行う。また、産業界・学術界と引き続き協力して信頼性の高い環境を研究開発の主要分野で整えるとともに、データや知的財産の盗難を防止する強固な手段を開発していく。

---

[26] マイクロプロセッサは、現在使われている多数の機器の頭脳にあたるものである。通信、防衛、医療等の重要分野と、主要産業の至る場所で使用されている。しかしシステム設計の技術的進歩は、現在、セキュリティと安全性の懸念のために滞っており、しかもシステムの複雑化がこの問題を悪化させている。

[27] デジタル省、5G Supply Chain Diversification Strategy（「5Gサプライチェーンの多様化戦略」）(2020年)

[28] 特に、先端ロボット、人工知能、通信、コンピューティングハードウェア、暗号認証、量子技術等、国家安全保障・投資法2021の指定分野に重点を置く。

デジタル・セキュリティバイデザイン

現在のサイバーセキュリティの脆弱性の70パーセントはマイクロプロセッサの設計上の欠陥にもとづいており、このことはすでに1970年代から知られている。このようなマイクロプロセッサは、テレビから電気通信に至るまで、あらゆるデジタル機器に搭載されている。政府はテクノロジーセクターと協力し、2025年までに新設計のマイクロプロセッサをスマートフォンやその他多数のデバイスに搭載できるようにしていく予定である。

マイクロプロセッサの設計を変えるには、グローバルなパートナーシップと投資が必要である。英国のリーダーシップのもと、政府による7000万ポンドの投資を通じて、将来はデバイスの設計にセキュリティが組み込まれ、サイバー攻撃が成功するリスクを大幅に軽減できるだろう。

この画期的な技術は、英国で研究・開発された。マイクロソフトやグーグル等の大手テクノロジー企業は、このセキュリティ上の新たな利点を自社製品に組み込むべく、投資を行っている。英国内の大学の研究者たちが、このセキュリティ技術の最善の利用方法の発見に取り組んでおり、政府は、国内中小企業がこの新たなセキュリティを組み込んだ製品の新市場を開拓する支援を行っている。

The Hut Group 研究開発担当ディレクター、フィル・ウィルソン

The Hut Groupは、急速に進化する消費財に重点をおいたeコマース企業です。当社が共通プラットフォーム上で運営するウェブサイトは200を超え、1分間に最大3000件の注文を処理しています。そのため、プラットフォームと顧客のセキュリティは当社の最優先事項です。どのようなサイバー攻撃も封じ込めることができるよう、多大な努力を注いできました。今後、当社システムにデジタル・セキュリティバイデザイン（DSbD）技術を導入する可能性にも大きな期待を寄せています。当社のシステムを、1億8000万ポンドの産官連携で開発されたこの新しいマイクロプロセッサで稼働すれば、システムのレジリエンスが向上します。とはいえ、新技術は当社の性能要件を満たさない限り採用することはできず、移行管理は複雑です。DSbDプログラムの最初の実証プロジェクトに参加できたことは光栄でした。近い将来、当社の全システムがこの新しいセキュリティの恩恵を受けられるようになることを望んでいます。

目的2a：
堅牢でレジリエントな国家的暗号キー（Crypt-Key）事業を継続していく。この事業は、英国政府の顧客、パートナー諸国、同盟国のニーズを満たすとともに、最強の敵対者からの脅威をも含めて最も重大なリスクを適切に軽減する実績をあげている。

137. 暗号キー（Crypt-Key）とは、英国政府が、政府、軍、国家安全保障関係機関にとって枢要となる重要情報およびサービスを、特に能力の高い敵対者からの攻撃対応も含めて保護することを目的に暗号を使用することを表現した言葉であり、国家安全保障と防衛能力の展開に関する英国の選択能力を支えるものである。世界をリードする暗号キー国家になるには、政府と民間の両方が適切なスキルとテクノロジーを有していなければならない。

138. 英国は、将来にわたって主権的暗号キーを開発できる数少ない国の一つであり続けるために、政府の能力への投資および国内暗号キー産業との協力を継続していく。また、キーマテリアルのサプライヤーであるNATOへの支援も含め、暗号キー分野のグローバルリーダーシップを今後も取り続けていく。それにより、国内の高スキル産業を支え、レジリエンスの高いエンジニアリングの強みを維持できるという二次的利益が得られるだろう。また、重要国家インフラ等の他の高保証コンテキストにも新しい堅牢な能力を実現する可能性がある。英国は2025年までに以下のことを実現する。

139. よりレジリエントでセキュアな英国暗号キーセクターが、持続可能で世界をリードする産業基盤に支えられている。これにより英国に必要なあらゆるソリューションが供給され、特定のパートナー諸国や同盟国への輸出も行われる。英国は、政府と産業界の能力および専門知識をより効果的に組み合わせ、厳格な国家的アプローチで暗号キー産業を管理していく。これによって、英国が必要とする明確な専門スキルを確実に育成することができるだろう。

140. 英国政府の暗号キーの能力とサービスが強化されており、英国と同盟国の絶えず進化するニーズを満たし、暗号キー開発の最先端に立ち続けることが可能である。英国は、ユーザーの要求を理解して中核的サービスを改善するために、強力な技術的指導力を発揮していく。ここには、キーマテリアルの提供や、製品・サービスの品質保証が含まれる。また暗号キーサービスを変革し、新テクノロジーを通じてより柔軟で目立たないものへとしていく。

141. 英国が暗号キー分野の世界的リーダーシップをいっそう推進し、パートナー諸国や同盟国への輸出を拡大している。英国は、ファイブ・アイズ、NATO、その他の国際的パートナーシップにおいてリーダーシップを維持しつつ、英国の暗号キー関連ソリューションの相互運用を可能にする、国際認定された標準の開発を推進していく。そして産業界との協力のもと、輸出の機会を最大化する。

目的3：
次世代のコネクテッドテクノロジーのセキュリティを確保しつつ、グローバル市場への依存で生じるサイバーセキュリティリスクを軽減し、英国のユーザーに信頼性の高い多様な供給へのアクセスを確保する。

142. 今後10年間、物理的物体やインフラ、そして長期的には人間自身をも含む人間の環境のより多くの部分に、コンピューティングパワー、インターネット接続、オートメーションが持続的に組み込まれていくだろう。そのため、サイバー空間の範囲が拡大し、生成されるデータの量も大幅に増加していく。従って、データを安全かつセキュアに管理する能力が、経済の安全な運営にとってこれまで以上に重要性を増していく。

143. 英国は、可能な限り、次世代のコネクテッドテクノロジーがセキュリティとレジリエンスを考慮に入れ、「セキュアバイデザイン」のアプローチを採用する協調的取り組みの一環として設計、開発、導入されるようにしていかなければならない。技術サプライチェーンのグローバルな性質により、技術依存のリスクをより積極的に管理するたには利用可能なすべての手段を用いていく必要がある。可能な限り、セキュリティがビルトインされるようにし、それが不可能な場合には、国内規制や標準に関する国際協力を含め、リスク軽減のための強固な手段を実施していく。英国は2025年までに以下のことを実現する。

144. 英国で販売される消費者向け接続可能製品が、必要不可欠なサイバーセキュリティ基準をクリアしている。英国で販売されるすべての新しい消費者向け接続可能製品に最低限のセキュリティ基準を課すことができるよう、製品セキュリティおよび電気通信インフラ法案（Product Security and Telecommunications Infrastructure Bill）を提出し、実施する。また、スマートで柔軟なエネルギーシステムへのサイバーセキュアな移行を支援していく（例えばスマートな電気自動車充電ポイントやエネルギースマートな家電製品等）。技術標準に関しては、標準化団体、産業界、パートナー諸国とも協力して、グローバルコンセンサスに影響力を発揮していく。さらに、英国の組織がより安全な方法でコネクテッドデバイスを調達、配備、管理できるよう、企業向けコネクテッドデバイスのための新しいセキュリティガイダンス等を通じてこれを支援する。

145. クラウド、ソフトウェア、マネージドサービス、アプリストア等のデジタルサービスの主要プロバイダーが、優れたサイバーセキュリティ基準に従うことを義務付けられ、組織と消費者をサイバー脅威から守るのに役立っている。デジタルサービスプロバイダーへの既存の規制を強化・拡大し、ICOの能力を向上させて、デジタルプロバイダーが自社サービス関連リスクをより積極的に管理するようにする。英国は、大手テクノロジー企業を含む産業界と引き続き協力し、市場の専門知識も活用して、英国のデジタル・サプライチェーンの安全確保に全員が役割を果たせるようにする。そして、デジタルサプライヤーに焦点を当てた国際的政策ソリューションの策定をリードしていく。

146. 英国が、コネクテッドプレイス技術の安全かつ持続可能な導入の最前線に立ち、国民と企業の利益となっている。スマートシティとも呼ばれるコネクテッドプレイスは、交通管理、汚染の削減、費用や資源の節約等、目に見える便益を社会にもたらす可能性を秘めている。しかし、場所の機能の効率化を可能にする相互接続性はまた、サイバーの脆弱性やサイバー攻撃の可能性を生み出すものでもある。英国は、NCSCのコネクテッドプレイスに関するセキュリティ原則に基づき、企業、インフラ、公共部門、市民に加わるリスクを削減していく。[29] また、地方自治体や、港湾、大学、病院等の組織がコネクテッドプレイス技術を安全に購入し使用できるよう、それらの能力を強化する。さらに、コネクテッドプレイスのセキュリティに関する一貫性のある効果的アプローチについて、国際的な合意を構築していく。

147. サイバーセキュリティが、英国で展開されている他の新興技術にも組み込まれている。英国は、サイバーセキュリティリスクを生む可能性のある新しい技術アプリケーションを特定し、そのような技術の安全かつセキュアな開発の最前線に立てるようにしていく。政府が、デジタルツインや広範な「サイバーフィジカルインフラ」技術における英国の能力に関するオプションを検討する際には、サイバーセキュリティが確実に意思決定の中心に置かれるようにしていく。[30] また、コネクテッドカーや自動運転車の幅広い展開においても英国が強固な地位に立てるよう、保証制度を確立していく。[31]

[29] 国家サイバーセキュリティセンター、Connected Places Cyber Security Principles（「コネクテッドプレイスのサイバーセキュリティ原則」）(2021年)
[30] Innovation Strategy（「イノベーション戦略」）(2021年)で発表。
[31] 安全・セキュリティ保証のためのコネクテッドカー・自動運転車プロセス (CAVPASS：Connected and Automated Vehicles Process for Assuring Safety and Security)

Angoka CTO・共同創設者、シャディ・A・ラザック

政府がセキュアなコネクテッドプレイスのガイドラインを発行し、自律走行車の利用がますます普及するに従い、社会におけるセキュリティの重要性が明らかとなっています。Angokaは、NCSCサイバーアクセラレータプログラムに参加したことを誇りとしています。当社は重要国家インフラから陸・空のモビリティまで、幅広い用途にソリューションを提供し、エンドツーエンドのレジリエンスとセキュリティ保証を実施してきました。

スマートシティやモビリティは複雑さを増し、コネクテッドデバイスやマシン間通信のネットワークへの依存を強めています。それらの安全性とレジリエンスを確保することが、当社のミッションです。当社のソリューションはトラステッドゾーンを生成し、分散型で耐量子性のあるセキュリティを運用します。これは攻撃者に動く標的を常時提供するためにダイナミックに更新されます。すなわち、デバイス所有者はセキュリティを完全にコントロールすることが可能です。

ソリューションのデモを行うAngokaのチーム

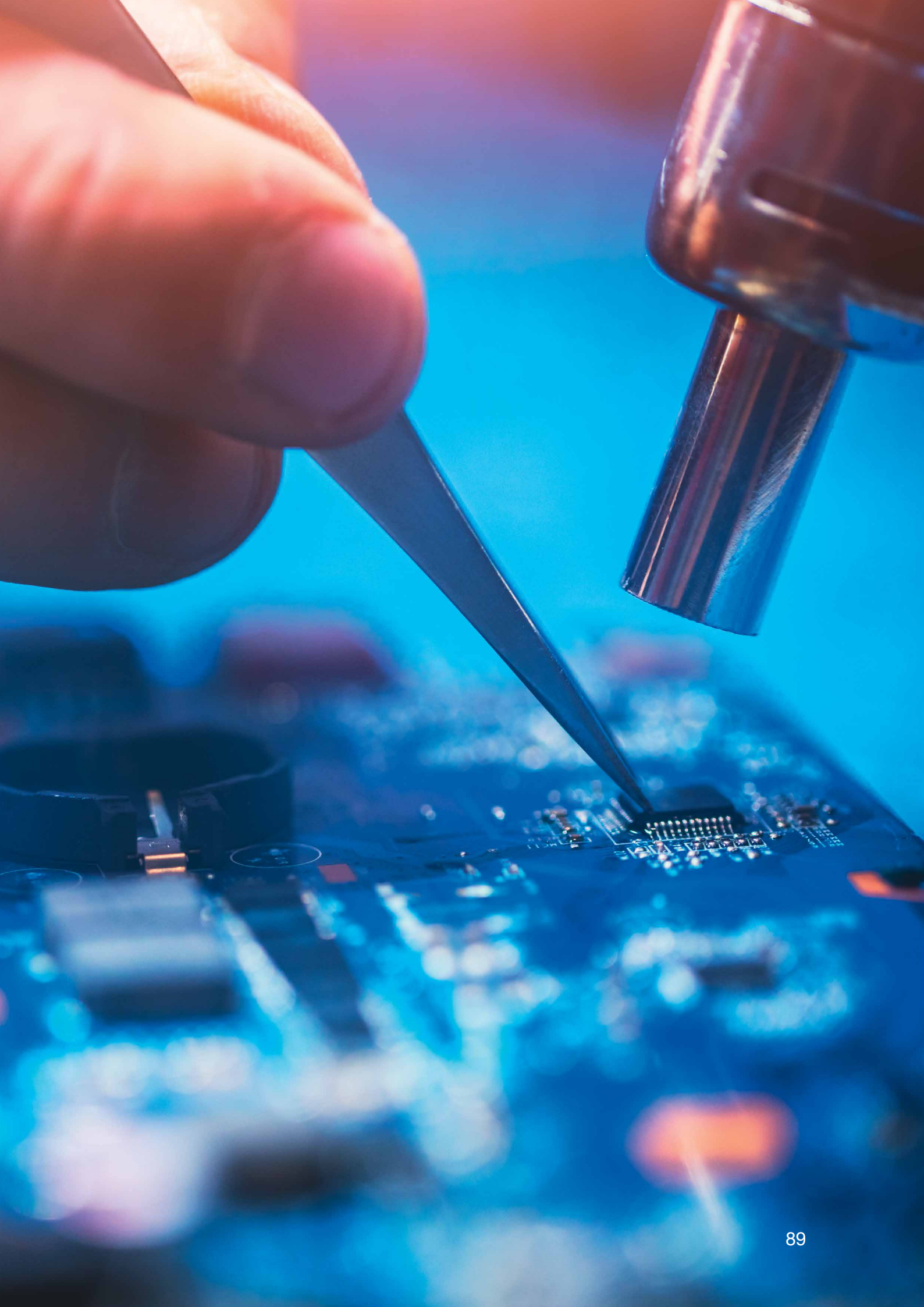
目的4：
マルチステークホルダーコミュニティと協力して、グローバルなデジタル技術標準の開発に寄与する。特に、民主主義的価値の擁護、サイバーセキュリティの確保、英国の科学技術を通じた戦略的優位の推進に関わる分野を優先する。

148. グローバルなデジタル技術標準は、インターネット、電気通信ネットワーク、新興テクノロジーの機能の中心的要素である。それがどのように開発され、展開されるかは、英国のサイバーセキュリティの目標、経済的繁栄、そして規範や価値観に影響を及ぼしうる。これまでこのような標準は最も市場力のある企業によって形成されてきており、実質的障壁の存在が中小企業や学術研究者、その他専門家を含む一部の重要ステークホルダーの参加を阻んでいる。英国は2025年までに以下のことを実現する。

149. グローバルなデジタル技術標準のエコシステムに、マルチステークホルダーが積極的に参加していること。英国は、重要な標準化団体へのマルチステークホルダーの参加を強化し、国際電気通信連合への英国代表団を通じて範を示していく。また、政策立案者にとっての重要な傾向や検討事項に関するオープンな議論を国連インターネットガバナンスフォーラムやその他のフォーラムを通じて促進する。さらにパートナー諸国との調整や情報共有も、英国がG7議長国を務めた時に設立されたデジタル標準ポイントオブコンタクト・グループ（Digital Standards Points of Contact Group）等を通じて強化していく。

150. 英国の優先分野におけるグローバルなデジタル技術標準が、民主主義的価値観、サイバーセキュリティへの考慮、新興技術における英国の研究およびイノベーションによって、より効果的に形成されていること。英国は、インターネットプロトコル、将来型ネットワーク、人工知能（AI）等の分野において産業界、学術界、技術専門家、市民社会組織と協力し、技術標準開発における重要な公共政策上の検討事項について啓発を行っていく。また、国家AI戦略で示しているとおり、AI標準化における英国のグローバルな関与を支援するためにAI標準化ハブを試験的に導入する予定である。

151. これらはすべて英国内の戦略的調整メカニズムによって支援される。例えばそれは国家AI戦略で定められた、政府、英国規格協会（BSI）、国立物理学研究所の間のイニシアチブ等である。このような関与はまた、イノベーションを可能にし成長と格差解消を促すような標準の推進を通じて、英国の繁栄を支えることにもなろう。



第4の柱：
グローバル
リーダーシップ

安全で豊かな国際秩序に向けて、英国のグローバルなリーダーシップと影響力を促進する

152. 自由でオープンで平和で安全なサイバー空間は、英国の集団安全保障と繁栄にとって極めて重要である。英国のサイバー戦略目標をすべて実現するには、国際的な関与が引き続き死活的に重要となろう。しかし、全システム的競争の時代への対応として、英国は今後、サイバー空間における国益と価値の増進のためにこれまで以上に積極的に国際指導力を発揮していく。英国のサイバー空間での活動やサイバーに関する専門知識は、政府の広範な外交政策課題を実現するうえでも中心的な役割を果たす。そのため、オープンで安全で繁栄する国際秩序の実現に向けて、これを積極的に役立てていく。

153. 英国は、中核的同盟関係を強化すると同時に、産業界、技術標準に関わる国際組織、市民社会組織、学術界を含む幅広いパートナーと協力しながら、問題解決力があり相応の負担を共有する国として活動していく。また、アフリカやインド太平洋地域のパートナー諸国との関係強化に投資し、新しく機敏性の高い提携の機会を捉えていく。さらに、外交的手段も継続的に強化し、海外での影響力と国内の強みを組み合わせながら、グローバルな利益の推進役として作戦や戦略上のコミュニケーション専門知識、各種スキルプログラム、経済パートナーシップを活用していく。英国のアプローチは、自国のみならず、世界の安全保障と繁栄に貢献するものである。

目的1：国際的パートナーのサイバーセキュリティとレジリエンスを強化し、敵対者を混乱させ抑止するための集団的活動を増強する。

154. 集団行動と相互的レジリエンスは、上流の脅威への対抗に不可欠であると同時に、サイバー脅威の行為者が英国とパートナー諸国を攻撃する誘因を引き下げることにもつながる。英国は2025年までに以下のことを実現する。

155. 英国のパートナー諸国が、サイバー脅威を調査・阻止し、レジリエンスを高めるために、優れた能力、政治的決意、ガバナンス、システムを手にしていること。
その結果として、英国民に対する海外からの脅威も減少する。英国は、東欧、アフリカ、インド太平洋地域においてサイバー能力の構築支援を優先的に実施するとともに、中東・米州の主要同盟国とも引き続き協力していく。また、より統合的で全政府的な技術提供を展開していくために、法執行および国防専門知識への投資を拡大し、英国産業界と学術界の活用もいっそう進めていく。その際、重要国際サプライチェーンおよびインフラの保護、デジタル技術の安全な利用の促進、産業界パートナーとの協力を通じた規模の拡大に、特に重点が置かれる。

156. 英国はまた、市民社会組織の能力を高めながら、テクノロジーと社会に関する価値主導の議論を促し、説明責任を果たせる地方レベルのメカニズムを打ち立てる取り組みを拡充する。そして、国連、ファイブ・アイズ、NATO、G7、欧州連合、英連邦、OECDや、サイバー専門知識に関するグローバルフォーラム（GFCE）、ASEANフォーラム、アフリカ連合、世界銀行等の効果的な多国間組織およびパートナーシップと、引き続き密に連携していく。

157. 海外における国益および国民の保護を強化するために、英国の在外公館を対象とする国際的なサイバー衛生キャンペーンを、現地の事情に合わせて開発し実施していく。その目的は、ハッキング、データおよびIPの盗難、ランサムウェア等の悪質な行為のコストを引き上げることにある。キャンペーンは、外交官、各国職員、現地英国企業、英国の開発プログラムの実施者を通じて展開していく。

158. 英国の敵対者に実質的責任を課す意思および能力をもつ、広範な国際同盟。
英国は、外交的関与、作戦協力、情報共有、共同演習の強化を通じて、国際的な決意と能力を向上させる。政策、運用、法執行のチャネルを通じて活動しつつ、標的型サイバー制裁等の措置の効果を高めるとともに、サイバー脅威の行為者のコストを引き上げる新たなツールを特定する。主要同盟国やパートナー諸国のサイバー部隊との相互理解を深め、陸、海、空、宇宙、サイバー空間の全領域において、サイバー作戦を同盟作戦に効果的に組み込んでいく。

159. 英国は、NATOの同盟としてのサイバーセキュリティ能力の開発を引き続き支援して集団行動の強化を図る。ここには、英国や他の一部の同盟国が自主的に提供する主権的なサイバー効果を、NATOの作戦やミッションに統合するプロセスへの支援が含まれる。

目的2：自由でオープンで平和で安全なサイバー空間を推進するために、グローバルガバナンスを形成する。

160. 英国の価値観を共有しない国は、自由で開かれたインターネットにある問題点を悪用し、サイバー空間の権威主義的ビジョンを安全保障を装って押し進めようとしている。国際的なルールや枠組みが英国の民主的価値観に沿って発展していくよう、英国は、同盟国やパートナー諸国と協力しつつ、より積極的なアプローチをとっていく。英国は、国内および世界の経済成長を支援し、集団安全保障を強化し、攻撃型サイバーツールの責任ある利用を奨励し、悪意のある無責任な活動に対して実質的責任を課していくことを目指す。英国は2025年までに以下のことを実現する。

161. 国際的ガバナンスおよび標準の枠組みの開発と実施に関して、**英国とパートナー諸国が影響力を増し、サイバー空間とインターネットのグローバルガバナンスが英国の利益と価値を守っている。**英国は、世界の経済成長と安全保障を推進するために、サイバー空間を統制する枠組みの形成に、より進歩的かつ積極的なアプローチをとっていく。サイバー空間におけるルール、規範、原則の適用に関する国際的議論を活発化させるための実務的手順を設計・実施し、破壊的で不安定な活動に対する効果的制約についてのコンセンサスへと、これをつなげていく。英国はこのことを、OSCE、ASEAN、GFCEを含む主要な地域的・専門的機関を通じて実施するとともに、ブダペスト条約と並ぶ新たな国際サイバー犯罪条約の策定に向けて、国際協力の強化と人権保護の維持を確保しつつ、国連のプロセスに建設的に関与していく。

162. 英国はまた、サイバー犯罪に関するブダペスト条約を引き続き擁護し、協力のための重要な国際協定としての正当性をパートナー諸国と協力しつつ主張していく。また、ICANNやインターネットガバナンスフォーラム（IGF）等の、インターネットのガバナンスのためのマルチステークホルダープロセスを引き続き推進し、強化していく。さらにこのような取り組みを補完するものとして、デジタル技術の世界標準の形成に努力するとともに（「技術的優位」の章で説明）、英国のサイバーセキュリティの輸出の拡大を図る（以下で説明）。それはまた、英国の基準を他国のサイバーエコシステムに定着させていくことにもつながる。

163. サイバー空間とインターネットの将来に関する英国のビジョンを中道的諸国の大半が支持・推進し、権威主義的国家がマルチステークホルダーシステムに及ぼす影響に効果的に対抗していること。英国は、権威主義的アプローチを採用せずにサイバー空間の課題に対処することが可能であることを実証し、同時にイノベーション、開発、成長を実現していく。他国への支援に関しては、国際的議論に参加し、合意された枠組みの実施に必要な法的・戦略的コミュニケーションの専門知識の全面構築を目的としてデジタル化に取り組む国々を支援する。また、サイバー能力を無責任に利用する者の暴露を続け、国際的信頼を構築していく。さらに、攻撃型サイバー能力の使用については可能な限りオープンかつ透明性の高いアプローチを示し続け、善を守る力（a force for good）としての英国の評判を固めていく。

目的3：英国のサイバー能力および専門知識を活用して輸出し、戦略的優位を高め、より広範な外交政策と繁栄のための利益を促進する。

164. 全システム的な競争と技術の急速な変化への対応として、英国のサイバー活動と能力は今後、国力のその他の源泉と並んで、戦略的優位を強化し外交政策と繁栄の諸目標を促進するものととらえられることになろう。英国は、開かれた社会と経済が繁栄し、人権が守られる国際秩序を実現すると同時に、自国の繁栄も推進していくことを目指す。英国は2025年までに以下のことを実現する。

165. サイバー空間内部またはそれに関連した英国の活動がグローバルな安定を強化し、ルールに基づく国際システム、開かれた社会、民主主義システムを、それが損なわれつつあるところで保護していること。英国は、サイバー空間の設計、開発、利用において人権、多様性、男女平等を擁護するために、価値観重視の国際的キャンペーンを展開していく。ここには、インターネットの遮断、人工知能のアルゴリズムのバイアス、オンラインの安全性向上への取り組みが含まれるが、それにとどまらない。英国は、民主主義の価値、システム、プロセスを守り、ルールに基づく国際システム（国連、世界保健機関、世界貿易システムを含む）の強化に向けて効果的に競争すべく、世界6大陸に広がるサイバー担当者ネットワークへの投資を増額する。また、英国の研究協力や学術交流プログラムを促進するための戦略的コミュニケーションの利用を強化するとともに、英国のアイデアを確実に実用化していく支援を行う。

166. 英国が、サイバーソリューションとサイバー専門知識の輸出大国として世界トップ3の位置に立つこと。英国サイバー産業を、サイバーセキュリティソリューションを求める世界各国の政府と主要な商業顧客にとっての第一の選択肢にしていく。英国は、サイバーセキュリティ・アンバサダープログラムおよび国際ネットワークの支援のもとに、政府間の国際協力の活発化を通じて、英国のサイバーセキュリティを最大限にアピールしていく。また、イノベーションから輸出に至るあらゆる段階で英国全土の企業を支援し、有力な輸出業者として対英投資を呼び込めるようにする。また、新しい輸出ファカルティ（Export Faculty）の創設等、中小企業への支援も強化する。[32][33] サイバー成長パートナーシップを通じた活動や、「サイバーエコシステム」の章で説明したその他の取り組みと並行して、新たにサイバー能力キャンペーン事務局も設立し、大々的な輸出キャンペーンを体系的かつ組織的に支援していく。

---

[32] UK Innovation Strategy（英国イノベーション戦略）(2021年)で説明。

[33] 英国の国防・安全保障輸出の振興機関であるUKDSEの輸出ファカルティは、防衛・安全保障セクターの中小企業を対象とするオンライン学習・開発ハブであり、サイバーセキュリティ企業向けの特別モジュールも用意している。ファカルティに登録すると、カリキュラムに基づく学習モジュールのプログラムにアクセスできるほか、UKDSEが運営するイベントや活動に関する有益な情報も得ることができる。

英国デジタルアクセスプログラム（ケニア・ナイロビ）チャールズ・ジュマ

私はチャールズ・ウェソンガ・ジュマと申します。サイバーセキュリティ、デジタル開発、インクルージョン、アントレプレナーシップを主導、形成、提供しています。これは、グローバルかつ政府横断的な英国デジタルアクセスプログラムのケニアにおける実施の一環です。また、紛争・安定・安全保障基金（CSSF）のサイバーポートフォリオに基づく様々な補完的プロジェクトも支援しています。オンラインの安全性、セキュリティ、データ保護、サイバー空間の責任ある利用の重要性は、いくら強調してもし過ぎることはありません。新型コロナ・パンデミックを教訓として、オンラインの安全性と衛生は、公衆衛生と同じくらい重要であると言えます。私は、英国政府の総合的サイバーパワーの任務を担う一人として、すべての人をオンラインの脅威や被害から確実に守ることに情熱を注いでいます。

在ジョージア・トビリシ英国大使館サイバー担当官　サラ・マーチャント

こんにちは、サラ・マーチャントです。英国大使館のサイバー担当官としてトビリシに赴任し、ジョージア政府および英国国家サイバー部隊センターと密に連携しています。日々の仕事は、政策への関与から、新サイバー戦略の実施支援、ジョージアの技術力改善のために英国の専門家を活用することまで多岐にわたります。英国の専門知識を発信し、ジョージアがサイバー脅威へのレジリエンスを高めるために支援するという業務の最前線に立っており、やりがいを感じています。残念ながら、敵対的国家活動の最先端に立たった経験が多い国として、ジョージアは数々の教訓を与えてくれます。私たちの業務により、ジョージアと英国がともにより強く、レジリエンスが高く、情報に通じた国になることを目指しています。

第5の柱：
脅威への対抗

英国の安全保障をサイバー空間の内部およびサイバー空間を通じて強化するために、敵対者を検知、攪乱、抑止する

167. 英国が直面している脅威は複雑な性質をもつ。懸念される脅威は、サイバー空間内部のもの（例えばオンライン活動への脅威）や、サイバー空間を通じて英国やパートナー諸国にもたらされるもの（例えばネットワーク化している英国の重要国家インフラへの脅威）のほか、基盤となる国際サイバーインフラ機能への脅威があげられる。これらの脅威はいずれも、人々が依拠する様々なサービスの可用性や、それらサービスのシステムを通過するデータ・情報の機密性または完全性に影響を及ぼす恐れがある。脅威に対抗するための英国のアプローチの基礎は、本文書で上述のとおり、サイバーレジリエンスの促進にある。本章では、サイバー空間で英国を攻撃するコストとリスクをどのように高めるか、また、サイバー大国としての潜在能力を最大限に発揮するにはどうすべきかに焦点を当てる。

168. 英国は、「国家サイバーセキュリティ戦略 2016-2021」の施行以来、脅威を軽減するためのアプローチを変革してきた。サイバー脅威の検知と分析に関しては、世界最高水準の能力を国家サイバーセキュリティセンター（NCSC）の構成要素として確立した。NCSCは、国内外の官民のパートナーと協力しつつ、脅威とインシデントを検知し、これに対処している。NCSCはまた、より広範な情報（インテリジェンス）コミュニティの一員として、英国の利益に対する攻撃の帰属に関して政策立案者に情報提供することが可能である。これは、英国のサイバー脅威抑止策の重要な要素である。攻撃型サイバー能力に対しても、国家攻撃型サイバープログラムや新しい国家サイバー部隊（NCF）を通じて多額の資金を投じてきた。また、国家犯罪対策庁（NCA）主導で統合的な国内法執行対応を展開し、サイバー空間における敵対的・犯罪的活動を攪乱し、そのコストを引き上げることを目指している。世界最高水準の脅威の検知・評価能力は、その結果得られる洞察を公民両セクターでインパクトのある緩和策にしていく手段とともに構築されている。さらに、自律的なサイバー制裁体制も構築し、敵対者にコストを課すもう一つの手段としている。英国の外交活動、国家サイバーセキュリティセンター、安全保障・情報機関、国家犯罪対策庁、法執行機関、国家サイバー部隊のすべてが一体となり、脅威がもたらす現実的影響を、敵対者への直接的対抗、攻撃回避、被害の抑制を通じて削減している。

169. しかし脅威もまた精緻化し、複雑さと深刻さを増している。様々な対策をとっても攻撃者のリスク計算を根本的に変えるには至っておらず、引き続き英国と英国の国益が標的にされている。英国に対するサイバー攻撃の動機となっているのは、スパイ活動や犯罪、商業的、金融的、政治的利益のほか、破壊工作、偽情報の普及である。攻撃者は緩和策を回避する能力を開発している。ますます精緻化するサイバーツールと関連イネーブラーが、成長産業において商品化され、あらゆるタイプの悪意ある行為者の参入障壁を低くしている。また、行為者が貴重なデータを盗んで暗号化し、ランサムウェアの支払いを強要する能力が高まるにつれて報酬も増加し、企業や重要公共サービスに混乱を引き起こしている。その結果、攻撃者が金銭的利益を得、プライバシーや言論の自由を侵害し、偽情報によって出来事を操作する傾向がますます強まっている。

170. したがって英国のアプローチは今後、敵対者にコストをかけ、実行犯を追跡・攪乱し、将来の攻撃を抑止することを目的に、利用できるあらゆる手段や能力を日常的、統合的、創造的に活用していくという、より統合された持続的キャンペーンへと移行していくだろう。このアプローチを支える重要要素として、以下のものが挙げられる。

- 敵対者に攻撃型サイバー作戦を仕掛ける英国の能力の次なる段階としての、国家サイバー部隊の継続的開発。
- 英国の脅威への対策として特別に策定する政府横断的キャンペーン（外交、軍事、情報、法執行、経済、法律、戦略的コミュニケーションの各ツールを活用）。
- 重大犯罪者とそれが依拠するサービスの阻止・発見を目的として、法執行機関が大規模かつ迅速に捜査を行い、敵に対する技術的優位を維持できるようにする新たな投資。
- 「レジリエンス」の章で説明のとおり、政府と産業界の間でのデータ共有の大幅拡充。

171. サイバー空間は英国にとっての機会であり、国益を積極的に追求する新しい方法を生み出している。例えば攻撃型サイバー作戦は、柔軟で拡張可能、なおかつデ・エスカレーション（段階的縮小）の効果を期待できる様々な手段となり得る。多くの場合、個々人を物理的な危険にさらす必要を避けながら英国が戦略的優位を維持し、国家的優先事項を実現するのに役立つものである。

172. 英国は、国家サイバー部隊を通じて、攻撃型サイバー能力の開発およびそれへの投資を続けていく。国家サイバー部隊は、英国と英国民、そして英国のやり方を守ることを目的として、英国がサイバー空間および現実世界で敵対者に対抗する能力を変革していく。このような能力は、外交、経済、刑事司法、軍事力と並んで、「善を守る力」として責任を持って使用される。また、国家安全保障、経済的福利、重大犯罪の防止および検知に関連する政府の幅広い優先事項を支援し、推進するためにも使用される。

目的1：
英国とその利益および国民を守るために、国家、犯罪者、その他悪意のあるサイバー行為者と活動を検知し、調査し、情報共有する。

173. 英国は2025年までに以下のことを実現する。

174. 政府が、外国国家、犯罪者、その他の悪意あるサイバー行為者のサイバー能力と、その英国に対する戦略的意図を包括的に理解している。英国は、2016年の前戦略のもとで実施された、サイバー脅威理解のための情報機関および法執行機関への多額の投資を維持し、拡大していく。特に法執行機関の能力を高めてサイバー犯罪の脅威の理解とそれへの対処を改善し（ここには、脅威と外国国家・その他国内外の脅威との関連性や、脅威の技術的イネーブラーも含まれる）、より効果的な政策対応の開発に役立てていく。また、情報機関と法執行機関を横断する共同データアクセスおよび活用戦略を打ち立て、政府全体で脅威の検知を調整する方法を改善する。さらに、敵対者の意図や意思決定基準、および英国の活動が敵対者に与える影響についての理解にも（個人がどのようにしてサイバー犯罪者になるのか、それを防ぐにはどうすべきか等を含め）、これまで以上に注力していく。

175. この成果を達成するには、「レジリエンス」の章で説明のとおり、サイバーインシデントおよび犯罪の迅速かつ容易な報告に向けた取り組みも役立つだろう。

176. あらゆる情報源を活用し、政府、法執行機関、民間セクター全体の専門知識を結集して、**最も深刻な国家的、犯罪的、およびその他の種類の脅威の日常的かつ包括的な調査を実施している。**英国は、法執行機関のサイバーネットワークの情報（インテリジェンス）、運用、技術の各能力を構築していく。今後の投資は、組織犯罪グループを標的とする国家犯罪対策のサイバー情報能力、英国全土の情報（インテリジェンス）へのアクセスおよび移動を強化する地域情報構築イニシアチブ、そして、法執行機関がサイバーおよびデジタル犯罪の捜査・攪乱のために必要とするスキルと能力に対して行っていく。

177. 捜査ではあらゆる情報源からの情報を支えとしつつ、民間セクター全体のスキルと知識も活用し、例えば企業による法執行機関とのデータ共有も円滑化していく。また、国、地域、地方レベルのサイバー犯罪ネットワークを安全に保つため、サイバー犯罪への警察対応に関するHMICFRSの勧告を引き続き実施する。[34]

[34] 英国警察庁・消防庁検査局（Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services）

178. 脅威に関する情報とデータが日常的に大規模かつ迅速に共有されており、受信者が行動に移す能力も向上している。 NCSCは、様々なセクターでネットワーク防衛者の効果的コミュニティを構築するために、幅広い取り組みを試みてきた。ネットワーク防衛者は、脅威に関する情報を受け取り、共有するばかりでなく、それを集団利益のために利用する能力もますます高めている。英国は政府サイバー調整センター（「レジリエンス」の章で説明）の支援のもとでこの取り組みを拡大し、まずは政府自身の自衛能力の向上に重点を置いていく。民間セクターではすでに、金融セクター・サイバーコラボレーションセンターが先導的役割を果たしている。[35]

179. NCSCはまた、新たな脅威の追跡方法を探っており、特定の種類のサイバー攻撃の検知に機械学習を活用する可能性について、アラン・チューリング研究所と協力しつつ引き続き調査している。この研究は、人工知能を使って悪意のある活動を検知する方法についても理解の向上をもたらすだろう。

[35] 国家サイバーセキュリティセンター、Financial sector cyber collaboration centre（「金融セクター・サイバーコラボレーションセンター」） (FSCCC) (2021年)

サイバー犯罪の阻止が可能にする、その他の犯罪行為への対処

サイバー犯罪（コンピューター不正利用防止法違反と定義される）は、コンピューター、ネットワーク、データ、その他デジタル機器への不正アクセス、それに伴う損害を生じさせる行為、または、これらの犯罪を行う手段の作成や提供により発生するものである。サイバー犯罪者はこのようなサイバー犯罪を通じて、ランサムウェア攻撃や、不正なアカウントアクセス、知的財産の盗難、サービス妨害攻撃、大規模な個人データの盗難といった悪意のあるサイバー行為をさらに実行できるようになる。これらの犯罪は重大であり、かつ拡大している。

一般市民にとって、サイバー犯罪は、それによって可能になり促進される更なる犯罪として現れることが多い。不正なコンピュータアクセスは様々な詐欺や窃盗、セクストーション（性的脅迫）を引き起こす可能性があり、場合によってはストーカー行為や家庭内暴力、ハラスメントを助長する。これらの犯罪は事業活動を破壊したり、生活を崩壊させたり等、いずれも日常的に英国市民に多大な被害を与えている。したがってサイバー犯罪は、より広範なオンラインの安全性に関する問題（いじめや嫌がらせ、ヘイトスピーチ、偽情報の拡散、ギャング文化や暴力の奨励、未成年者のポルノへのアクセス等）とは区別される異種の犯罪である。政府は現在、オンライン被害白書およびオンライン安全法案の作成を通じて、これらの問題に取り組んでいる。

目的2：
英国とその利益および国民を狙った、国家、犯罪者、その他悪意のあるサイバー行為者と活動を抑止し、攪乱する。

180. 英国は2025年までに以下のことを実現する。

181. 外国国家、犯罪者、その他の悪意のあるサイバー行為者にとって英国を標的にすることのコストおよびリスクがこれまで以上に高くなっていること。英国は、悪意のある犯罪的サイバー行為者の行動に影響を与えるために、あらゆる能力（外交的、経済的、および秘密・明白の両手段を含む）を活用して持続的かつ個別適応型の抑止キャンペーンを展開する。特に、英国が敵対者に有意なコスト（制裁や、法執行機関・国家サイバー部隊の活動を通じたものを含む）を課す能力と意志をもつことを、敵対者に対して強力に伝えていく。また、国家サイバー部隊のサイバーチョイス（Cyber Choices）プログラムを通じて、個々人がサイバー犯罪に巻き込まれることのないよう誘導していく。その際、産業界や学術界と協力し、潜在的犯罪者に実習制度や就職斡旋等のより良い選択肢を提供する。

182. 英国はまた、法執行機関と情報機関が必要とするツールと権限を、国家的脅威対策法案（Counter State Threats Bill）を通じて提供し、国家的脅威の進化を考慮しつつ既存の法律を更新するとともに、新しい犯罪を導入していく。さらに犯罪収益法2002（Proceeds of Crime Act 2002）を改正して、法執行機関がサイバー犯罪の収益を特定、押収、回収する能力を最適化する。そのために特に、起訴することのできない犯罪者がもたらすリスクを軽減するための民事没収権を創設する。

183. 外国国家、犯罪者、その他の悪意のあるサイバー行為者の活動や能力を英国が攪乱および削減し、その結果としてそれらの者が英国を標的にしにくくなること。英国は、ランサムウェアに関する政府の政策および運用のアプローチを見直してこれを優先的キャンペーンの一つにするとともに、産業界やパートナー諸国とも協力していく。国家サイバー部隊、国家サイバーセキュリティセンター、国家犯罪対策庁と、広範な法執行機関および外交・情報機関の間のパートナーシップを最大限に活用し、サイバー空間の機密性、完全性、可用性、あるいは、サイバー空間内のデータやサービスを破壊する脅威に対抗していく。特に、サイバー犯罪のインフラを標的にする能力に投資して、悪意のあるサイバー活動を攪乱するための法執行および攻撃型サイバー能力を展開していく。英国の敵対者はサイバー能力を高め、悪意のある目的のためにますますそれを使用するようになっている。そのため、適切と判断できる場合には、国家サイバー部隊をフルに活用し、こうした活動を妨害して英国を防衛・保護していく。

184. 英国はまた、ハイエンドなサイバー能力が外国国家や組織犯罪集団へと、商業・犯罪市場を通じて拡散していくことに対処するため、サイバー犯罪を可能にし、促進し、もしくは美化するようなフォーラムに対処していく。

185. サイバー犯罪者への刑事司法の適用およびその他攪乱による成果を増大させること。そのために、英国内のサイバー犯罪者を訴追する刑事司法の機能を改善していく。英国は、コンピュータ不正使用防止法と関連する権限を見直して、法執行機関が犯罪者の新たな脅威を調査する能力を確保するとともに、増加するサイバー事件に対処できる専門性の高い検察官を増やしていく。また、必要なサイバー専門知識を持つ警察官を継続的に確保するために、全国警察本部長会議（NPCC）のサイバー技能プロスペクタスや警察学校のサイバーデジタルキャリアパスを通じて、法執行の専門技能、演習、主流化を推進していく。

北アイルランド警察（PSNI）犯罪防止担当官　スーザン・ムーディ

（左から）スーザン・ムーディ（PSNI）、セーラ・トラヴァース（TVプレゼンター）、ジョー・ドーラン（北アイルランド・サイバーセキュリティセンター責任者）

コンピューターや携帯端末は若者の日常生活の一部となっており、大きなチャンスを与えてくれる一方、使い方を誤れば危険も生じます。PSNIの犯罪防止機能では、青少年への早期介入を実施し、コンピュータの使用と悪用に関する法律を理解してもらう手助けをしています。犯罪行為につながりうる危険な兆候に注目しつつ、サイバーファースト（CyberFirst）等の取り組みやサイバーを職業選択の一つにすることを通じて、大きなチャンスがあることも伝えています。好奇心や才能がある若者に犯罪以外の選択肢を示すとともに、それ以外の人たちが犯罪目的で悪用することを防止しています。スーザン・ムーディは、すべての中学校で利用できる学校向けサイバー情報プログラムの開発に精力的に取り組み、40以上の小学校と多数の中学校、そして青少年団体や各種コミュニティグループとも直接的な関わりを持ってきました。若者は英国の未来のサイバー大使や防衛者へと成長していく可能性があります。

目的3：国家安全保障と重大犯罪の防止・検知を支援するため、サイバー空間の内部およびサイバー空間を通じた対策を実行する。

186. 英国は2025年までに以下のことを実現する。

187. 英国のサイバー能力が、サイバー以外の脅威の抑止・妨害にも威力を発揮している。英国は、国家サイバー部隊を拡充し、この重要機能の長期ビジョンを実現する。その際、政府通信本部、国防省、秘密情報部、国防科学技術研究所と全面的に統合して、法執行機関や政府全体と密接に協力する。国家サイバー部隊は、合法かつバランスのとれた攻撃型サイバー作戦を実施する機関であり、サイバー空間で責任ある行動をとって範を示す。攻撃型サイバー作戦は、防衛・外交政策を含む英国の国家安全保障、および重大犯罪の防止を引き続き支援していく。

188. また、インフラや暗号通貨に対する法執行機関の技術的能力も拡充し、これを他の脅威に対しても展開できるようにする。

189. 「統合作戦概念 2025」に従い、**英国のサイバー能力が防衛作戦の全領域に統合されている。**[36] これにより、英国が敵対者に対して競争力の高い戦力を維持することが可能となり、同盟国やパートナー諸国の協力関係の強化にもつながる。また、国防多領域統合変革プログラム（Defence Multi-Domain Integration Change Programme）を引き続き推進して領域間の能力を一つにまとめ、国力を支える他の手段との統合を進めるとともに、敵対者に対する英国の軍事的優位を強化していく。サイバーは、高スキルをもつサイバー専門家と、国防職員全体の高いサイバー意識、そして最先端のレジリエントなサイバー能力により、国防事業の主流となっていくだろう。

[36] 国防省、Integrated Operating Concept（「統合作戦概念」）(2020年)

法執行機関による主なサイバー犯罪捜査事例

インペリル作戦（Operation Imperil）：
サイバー攻撃被害者の個人情報や銀行情報を販売していたウェブサイトについて、南東地域組織犯罪対策ユニット（SEROCU）がFBIと共同で実施した作戦である。当該ウェブサイトは、個人情報を他人が購入して詐欺やその他のコンピュータ不正利用犯罪を行うことを可能にしていた。大規模な調査により、技術インフラとして使用されていた銀行口座と支払履歴を特定することができ、ウェブサイトの所有者がパキスタンに拠点を置くことも突き止めた。その結果、FBIはウェブサイトを秘密裏に押収し、その後削除することができた。南東地域組織犯罪対策ユニットは、犯罪資金の洗浄を目的にウェブサイト所有者に代わって米国に銀行口座を開設していた英国内の主犯を逮捕した。この容疑者は、漏洩した被害者情報の一部を利用して多額の詐欺を行い、別名で複数の銀行口座を開設していた。また、漏洩した銀行口座を利用して豪華な休暇の支払いや労働年金省に対する虚偽の請求を行い、9万ポンドを超える損失を国にもたらしていた。容疑者は9つの訴因で起訴され、早期有罪答弁により4年に短縮された懲役刑を言い渡された。なお捜査チームは裁判官より裁判官表彰を授与された。本文書発行時点では、没収、および生涯的な犯罪収益法（Proceeds Of Crime Act）の適用が進行中である。

ニピゴン作戦（Operation Nipigon）：
ブルガリア国籍の男が特注のフィッシングページを作成し、英国に推定4000万ポンド超の損害を与えた容疑でロンドン警視庁が捜査した。容疑者の特定は、容疑者が作成したフィッシングページを使って独自に犯罪を行っていた別のサイバー犯罪者の捜査から実現した。よく知られていたこの犯罪者は、2018年に10年の懲役刑を言い渡されていた。捜査は、ある重要なメールアドレスが容疑者に関連していることが判明し、開始された。多くの長期的かつ複雑な調査を経てブルガリア当局の協力が得られ、容疑者は逮捕、送還された。包括的な情報開示の後、容疑者はすべての刑事責任を認め、9年半の懲役刑が確定した。

リーシング作戦（Operation Leasing）：
新型コロナ・パンデミックさなかの2020年、国家犯罪対策庁は、ビットコイン（BTC）の支払い要求に応じなければ爆破するとNHSを恐喝したテロリストの捜査を主導した。ドイツ当局との協力を得て特定、逮捕した容疑者は、ドイツの裁判所で有罪判決を受けた。

2020年4月12日、イタリア国籍のドイツ在住者が、ビットコインで1000万ポンドを受領しなければNHSの病院を爆破するという内容のメールを、TORネットワーク経由で送信した。

国家犯罪対策庁はこれを直ちに最優先事項として特定し、サイバー犯罪専門担当官が犯人捜査と潜在的攻撃の防止に当たった。

犯人は以前より、国会議員の攻撃やロンドンのブラックライブズマターのデモ参加者の爆撃を予告する脅迫メールを送っていた。犯人のメールは英語で書かれていたが、国家犯罪対策庁捜査官は特殊なサイバー技術と行動・言語分析を利用して、犯人はドイツ語を母国語とする人物であると推論した。

そこで、ドイツ当局と協力し、メールがベルリンの住所にあるコンピューターから送信されていることを突き止めた。容疑者は身元と場所を隠すために様々な策を講じていたが、国際協力を通じて特定することができ、ドイツの法執行機関の監視対象とすることが可能となった。2020年6月15日に同容疑者は逮捕され、恐喝未遂の罪で告発、拘留された。その後2021年2月26日に有罪判決を受け、3年の懲役刑に処せられた。

サイバー空間を通じたテロ対策の実施

反ダーイッシュ・キャンペーン：国防省と政府通信本部の対イスラム国（ダーイッシュ）活動は、インターネットと現代の通信の力を悪用する者からの脅威に対する英国の積極的対抗策の好例である。

イスラム国はテクノロジーに多くの時間とエネルギーを費やし、人々を過激化して勧誘し、テロ攻撃を鼓舞するメディアコンテンツを制作している。近年は、ロンドンやマンチェスターでのテロを含め、欧州全体でこの手法の影響が明らかとなっている。イスラム国はまた、最新の通信システムを使って戦場での作戦を指揮・統制してきた。それによって柔軟な活動を大規模かつ迅速に実行することが可能であり、支配を目論む地域の住民にさらに大きな危険をもたらすとともに、いわゆるカリフ全体に最大限の影響力を及ぼすことが可能だった。

イスラム国の首都と宣言されたモスルの戦いで、英国は、連合軍の支援および広範な全面的キャンペーンの一環として、軍とともにサイバーツールおよび技術を使った作戦を展開した。その成果は多岐に及んだ。通信の遮断、プロパガンダの弱体化、グループ内の不信感の醸成、作戦に使用する機器やネットワークの遮断等、いずれもイスラム国の実効性の低下につながる事態であった。英国はまた、サイバー技術を利用してターゲット集団に英国政府のメッセージを伝えたり、無自覚にイスラム国を支援する可能性のある人々にその活動を明示したりすることができた。これらの作戦はイスラム国のプロパガンダを抑える連合軍の努力に大きく貢献するとともに、イスラム国の攻撃調整能力を妨げ、戦場で連合軍を守ることにも役立った。

国家サイバー部隊メンバー
アンドリュー

私はこれまで常に最先端のテクノロジーに関心をもってきました。諜報機関の前は警察で働いており、巡査の職に始まって、その後、容疑者の電子機器を調べて証拠をつかむデジタルフォレンジックの専門職に昇進しました。その仕事は好きでしたが、他にも機会がないかと考えて今の職に就きました。

私は大学には行かず、元々の好奇心からキャリアを築きました。サイバー部隊の同僚についても同じことがいえ、皆、実に様々なバックグラウンドの持ち主です。根っからのテクノロジー専門家もいれば、元スーパーの店長や、小学校の先生、消防士等、いろいろです。ただ共通しているのは、オープンマインドであり、学ぶ意欲があって、国の安全を守るという目的を共有していること。新しいテクノロジーが国家安全保障に対してもつ脅威と機会に注目しています。

警察官時代は、一個人のレベルで人助けができることに誇りを感じていました。現在は国家サイバー部隊というユニークなチームの一員として、グローバル規模で「善の守る力」の一翼を担っています。

英国の野心的目標を実現するために

190. 本戦略が意味をもつには、目標実現のための厳密な方法、進捗状況のモニタリングと評価、そして必要に応じて軌道修正するメカニズムが不可欠である。本章では、実行のためのアプローチについて説明する。

政府全体の役割と責務

191. 国家サイバー戦略は今後、統合レビューの野心的目標を集合的に実現するための下位戦略の一つになる。これらの戦略を閣僚レベルで監督するのは国家安全保障会議であり、これが実施状況の監視と、英国の戦略の全体的バランスおよび方向性を検討する。また、戦略目標に対する進捗状況は、政府の計画・実績フレームワーク（Planning and Performance Framework ）および成果実現計画（Outcome Delivery Plans）を通じて評価される。

192. すべての閣僚は、英国が責任ある民主的サイバー大国としての地位を固め、自国の利益をサイバー空間の内部およびサイバー空間を通じて保護し促進できるようにする役割を担う。以下に示すのは、国家サイバー戦略の5つの柱のうちの一つ以上の実施・調整、あるいは、最重要サイバー能力および政策決定の監督に主導的役割を果たす各閣僚の具体的な責務である。

- **ランカスター公領大臣**は、**財務省主計長官**の支援を得つつ、サイバー脅威への政府の効果的対応およびサイバー大国としての野心的目標の実現に向けて、省庁横断的な全体的リーダーシップをとる。ここには、国家サイバー戦略の策定と実施、投資プログラム支援、サイバーレジリエンス関連諸政策の調整が含まれる。また、英国の重要国家インフラのサイバーセキュリティおよびレジリエンスに関しても、セクター横断的な政策および調整の全体的責任を担う。サイバーインシデントに関する閣僚級のCOBR

ミーティングが必要な場合は、ランカスター公領大臣が既定の議長として参加する。

- **内務大臣**は、国家サイバー戦略の全体的な実施、および国土安全保障責任に沿ったサイバーインシデント対応において重要な役割を担う。敵対者の検知、攪乱、抑止のための政府の活動を外務大臣・国防大臣とともに主導し、その全体的な調整も行う。また、サイバー犯罪に対抗するための具体的責任も負う。

- **外務大臣**は、GCHQと国家サイバーセキュリティセンターに対して法的責任を負う。英国のサイバー分野でのグローバルリーダーシップを推進する政府の活動を主導するとともに、サイバー帰属プロセス、サイバー制裁体制、および高カテゴリーのサイバーインシデントへの国際的関与に対して特別な責任を負う。また、敵対者の検知、攪乱、抑止のための政府の活動を内務大臣・国防大臣とともに主導する。

- **国防大臣**は、外務大臣・内務大臣とともに、敵対者の検知、攪乱、抑止のための政府の活動を主導する。

- **外務大臣および国防大臣**は、国防と情報（インテリジェンス）間の共同努力としての国家サイバー部隊に責任を負う。

- **デジタル・文化・メディア・スポーツ大臣**は、経済全体の様々な組織のサイバーセキュリティを、デジタル政策や関連分野の成長、および国家サイバー戦略のイノベーションとスキルの要素に関係するものとして主導する。また、英国のサイバーエコシステムを強化し、サイバーパワーとして不可欠な技術で主導権を握ることができるよう、政府の活動をリードしていく。

- **重要国家インフラを管轄するすべての主導的政府省庁の大臣**は、それぞれの管轄セクターのサイバーセキュリティおよびレジリエンスに関する政策に対して責任を負う。

- **すべての閣僚**は、それぞれの省庁のサイバーセキュリティを監督し、適切な緩和策を実施しなければならない。ある部門が公共・民間部門を監督する場合は（例えばDLUHCと地方自治体、DEFRAと水道会社等）、当該セクターに関連するサイバー政策および保証活動にも責任を負う。

193. 本戦略の上級責任者は情報（インテリジェンス）・安全保障・レジリエンス担当の副国家安全保障顧問（Deputy National Security Adviser for Intelligence, Security and Resilience）であり、各省庁の関連高官の支援を受けつつ、公式レベルで政府全体の実施を主導する。

国家サイバー戦略

閣僚の責務

* サイバー脅威への政府の効果的対応、および、サイバー大国としての野心的目標の実現のために省庁を横断して総合的リーダーシップをとる。

英国のサイバーパワーへの投資

194. 政府は今後3年間に、サイバーおよびレガシーITに26億ポンドを投じる予定である。これは、国家サイバー部隊への多額の投資とは別に実施される。新たな投資には、国家サイバーセキュリティプログラムへの1億1400万ポンドの増額が含まれる。また、2016年戦略に基づき構築された能力への年間支出を政府省庁の管理下に移し、恒久的な歳出とする。さらに、パートナー諸国を支援し、サイバーレジリエンスを構築し、サイバー脅威に対抗するための国際的なプログラムも、紛争・安定・安全保障基金（CSSF）を通じて実施していく。これは、研究開発、情報（インテリジェンス）、防衛、イノベーション、インフラ、スキルへの投資増額と並ぶもので、いずれも英国のサイバーパワーの一翼を担うことになる。[37]

成果の測定

195. 本戦略の管理は、上級責任者と国家安全保障会議の監督の下に置かれる、継続的に進化するパフォーマンスフレームワークによって行われる。同フレームワークは、英国議会、および国家安全保障関連活動を監督する他の機関との議論に情報提供するものとして活用される。「国家サイバーセキュリティ戦略 2016-2021」のアプローチと同様、同フレームワークは機密情報が含まれるため公表はされないが、政府が年次進捗報告書を公表する。

196. パフォーマンスフレームワークは以下のことを行う。

- 各活動が本戦略で示す多種多様な目標にどのようにつながっていくのか、明確な道筋を示す。
- 本戦略の実現に向けてアカウンタビリティを確保する。
- 本戦略で定める目標に向けた国の進捗状況に透明性を与える。
- 各活動が本戦略に沿ったものとなるには、どのような適応が必要かを明らかにする。
- 戦略目標を達成するにはどのような活動が効果的であるかを理解し、得られる教訓を今後に活かせるようにする。
- 5つの柱の活動を全体的見地から把握し、重複を減らして、国のサイバーパワーの強みと弱みを明らかにする。
- 本戦略が社会の全部分にサイバー支援を提供するよう確実にする。

[37] 財務省、Autumn Budget and Spending Review 2021（「2021年秋期予算及び歳出レビュー」）(2021年)

今後のステップ

197. 本戦略は、サイバーとその他広範な関連政策（付録Aを参照）に責任を持つ政府関係者だけでなく、英国のサイバー政策に関心と責任を持つ全社会のすべての個人と組織のための行動指針となることが意図されている。また、今後5〜10年間に英国の目標や優先事項を引き続き適切なものにするべく、今後継続的に行っていく議論の最初の一歩でもある。本戦略の公表を、英国全土の公民および第三の全セクターとさらに協力関係を築いていくための出発点としたい。（ご意見・ご感想をぜひこちらまでお寄せください：ukcyberstrategy@cabinetoffice.gov.uk）本戦略の実行についての進捗状況は、毎年報告していく予定である。

付録 A：政府の広範な政策課題の一部としてのサイバー

国家サイバー戦略は、安全保障、防衛、外交政策、経済政策等の、政府の他の様々な優先課題を支援し、拡充することを意図している。そして本戦略は、英国の教育・職業訓練制度を通じて開発される広範な能力と、デジタルおよびテクノロジー産業政策、研究、ビジネスの成長に関する国家的アプローチに依拠するものとなる。関連性の高い重要戦略および計画は次のものが含まれる。

- **統合レビュー**。レジリエンスの改善や、国家的脅威、深刻な組織犯罪、テロリズムへの対処、科学技術を通じた戦略的優位の維持、そして国際秩序の形成を目指す様々な国家的取り組みを扱っている。
- **国家データ戦略**。英国のビジョンとして、責任あるデータ利用の力を活かして生産性を高め、新しいビジネスと雇用を創出し、公共サービスを改善し、社会の公正化を支援し、科学的発見を推進して、英国を次のイノベーションの波の先駆者に位置づけることを目指す。ここには、政府のデータ利用を変革して効率化を促進し、公共サービスを改善するため、省庁間のデータ共有の障害要因に対処するとともに、保有するデータの質を高めることが含まれる。このことは英国のサイバー政策課題、例えば、サイバーインシデントに関する良質のデータを収集・利用できるようにするといった課題を支援していくうえで不可欠である。
- **成長のための計画**。これはパンデミック後の復興政策である**「ビルド・バック・ベター」(Build Back Better)**を、インフラ、スキル、イノベーションへの追加支援・投資を通じて実現するための計画である。また、**イノベーション戦略**は、イノベーション主導経済を打ち立てる野心的目標を設定している。
- **デジタル規制のための計画**。イノベーション重視のアプローチでデジタル技術を規制し、それにより繁栄を実現し、デジタル技術利用への信頼も構築していくことを目指す。
- **国家AI戦略**。来るべきAIの変革の10年に備えるため、AIエコシステムの長期的ニーズに投資し、AI活用経済への移行を支援するとともに、英国がAI技術の適正な国内的・国際的ガバナンスを実現することを目指す。ここにはまた、AI活用システムのサイバーセキュアなイノベーションを支援しつつ、国民を保護してその利用への信頼を築くための施策も含まれる。
- 近日公表予定の**国家レジリエンス戦略**。英国が今後どのように技術的脅威を克服し、サイバー空間でのレジリエンスを維持していくかについて重点的に取り上げる。
- 近日公表予定の**デジタル戦略**。デジタル変革への新たな意欲の広まりを活用し、成長を加速し、将来に向けて包括的で競争力のある革新的デジタル経済を構築し続けるという政府の明確かつ野心的なビジョンを説明。DCMSの「10の技術的優先課題」(Ten Tech Priorities)に基づいてデジタル分野における政府の目的をさらに設定する。
- **ネットゼロ戦略**。イノベーション主導で繁栄する英国経済を低炭素にすることを目指す。
- **犯罪撲滅計画**。刑事司法制度への信頼を回復し、犯罪と被害者を減らし安全な英国という共通ビジョンを実現する方法を定めている。[38]

[38] 内務省、Beating Crime Plan(「犯罪撲滅計画」)(2021年)

国家サイバー戦略を直接支援するのが、同戦略の個々の部分の達成方法を具体的に示す以下の2点の公刊物である。

- 近日公表予定の**政府サイバーセキュリティ戦略**。国家サイバーセキュリティ戦略の支援にあたって、政府と公共部門のセキュリティを改善するための具体的諸計画を設定する。
- 近日公表予定の**インセンティブ・規制レビュー 2021**。これまでの経済全体のサイバーセキュリティ向上に向けた取り組みがどのような効果を上げてきたかに関する調査結果と、レジリエンス構築を目指す柱のもとで企業と組織に関わる要素をどう実施していくかについての提案を示す。

付録B：NIS規制 — 国家戦略

イントロダクション

NIS国家戦略

1. 国家サイバー戦略は、「英国ネットワーク・情報システム（NIS）規制 2018」の規制2において、英国の国家戦略として指定されている。

2. 本付録に示すのは以下の詳細情報である。

- 英国内のNIS実施に責任を持つ主な機関の役割と責務。
- 関係する主要官庁一覧。

英国のNIS規制

3. 2016年に欧州委員会は、欧州連合（EU）におけるネットワーク・情報システムのセキュリティ強化を目的とした指令に合意し、英国政府もこれを支持した。

4. 2018年4月20日に政府は新たに「ネットワーク・情報システム（NIS）規制 2018」を議会に提出し、同規制は2018年5月10日に施行された。

5. NIS規制が定めた英国内の新たな規制体制枠組みでは、指定の基幹サービス運営者（OES）と関連デジタルサービスプロバイダー（RDSP）に対して、ネットワークおよび情報システムを保護するための技術的・組織的措置の実施を義務付けている。

6. 適用対象となるのは、英国経済と社会にとって死活的重要性があり、ネットワークおよび情報システムに大きく依存するエネルギー、運輸、飲料水、医療、デジタルインフラの各セクターである。

7. また、重要デジタルサービスプロバイダー（検索エンジン、クラウドコンピューティングサービス、オンラインマーケットプレイス）も適用対象である。

8. NIS規制は以下を定める。

- 実施の支えとなる**国家的枠組み**。国家戦略もここに含まれる。
- 規制当局として機能する、セクター別の**所轄官庁**
- **シングルポイント・オブ・コンタクト**（SPOC）としての国家サイバーセキュリティセンター（NCSC）、および、**コンピューターセキュリティインシデント対応チーム**（CSIRT）。

9. 進捗評価は、2〜5年ごとに「実施後レビュー」によって行う。

主な役割と責務

国家的枠組み

10. 内閣府は、NIS国家戦略を構成する国家サイバー戦略に責任を負う。内閣府はまた、重要国家インフラのセキュリティおよびレジリエンスの改善に対しても全体的責任を担う。

11. デジタル・文化・メディア・スポーツ省（DCMS）は、NIS規制の全般的な実施について、関連機関とNCSCの調整も含めて責任を負う。また、英国全体での広範なNIS実施を支援するため、各所轄官庁向けのガイダンスを発行する。

シングルポイント・オブ・コンタクト（SPOC）

12. NISに関する国際（EU）パートナーとの協力のための国家的窓口であり、行動や情報の要請を調整し、年次インシデントデータをまとめる。国家サイバーセキュリティセンターは英国のSPOCである。

コンピューターセキュリティインシデント対応チーム（CSIRT）

13. 国家サイバーセキュリティセンターは英国のCSIRTである。国家レベルのサイバーセキュリティインシデントの監視に責任を負う。リアルタイムの脅威分析、国家的サイバー攻撃に対する防御、技術的アドバイスの他、大規模サイバーインシデントが発生した場合は被害を最小限に抑えるための対応を行う。

14. 国家サイバーセキュリティセンターは、成果ベースのサイバー評価フレームワーク（CAF）を管理し、サイバーセキュリティに関する広範なガイダンスを国家技術当局として提供する。

所轄官庁

15. 所轄官庁はそれぞれの分野におけるNIS規制の監督と執行に責任を持ち、NIS規制の要件に基づきOESとRDSPのコンプライアンスについて指定および評価を行う。それらはNIS規制のスケジュール1で設定されており、一覧はセクション3に記載している。

基幹サービス運営者（OES）と関連デジタルサービスプロバイダー（RDSP）

16. 当該セクターの指定基準を満たすか、もしくは、NIS規制8（3）に基づき関連当局の指定を受けたOESまたはRDSPは、NIS規則の要件を順守しなければならない。

17. それには以下が含まれる。

- ネットワークおよび情報システムのセキュリティに及ぶリスクを管理するために、適切でバランスの取れた技術的・組織的対策をとること。
- ネットワークおよび情報システムのセキュリティに影響するインシデントのインパクトを防止し、最小限に抑えるために、適切でバランスの取れた技術的・組織的対策をとること。
- それぞれのサービスに重大な影響をもたらしたインシデントについて、関連する所轄官庁に通知すること。
- NIS規制に基づく検査要件を満たすこと。
- 情報、執行、罰則の通知に従うこと。
- また、RDSPは情報コミッショナー事務局（ICO）への登録が義務付けられている。

その他の関係官庁

18. 英国政府はNIS規制の実施において、国内自治政府および主要政府機関（Lead Government Departments）を含むその他の関係官庁と密接に協力する。

19. 国家インフラ保護センター（CPNI）は、関連する物理的・人的セキュリティに関するアドバイスを提供する。

NISの実施に関わる重要官庁一覧

国家機関	
英国NIS規制	デジタル・文化・メディア・スポーツ省
英国国家サイバー戦略	内閣府
英国シングルポイント・オブ・コンタクト（SPOC）	国家サイバーセキュリティセンター
英国コンピューターセキュリティインシデント対応チーム（CSIRT）	国家サイバーセキュリティセンター

所轄官庁					
セクター	**サブセクター**	**イングランド**	**ウェールズ**	**スコットランド**	**北アイルランド**
エネルギー	電力	共同管轄：ビジネス・エネルギー・産業戦略省と、ガス・電力市場局（Ofgem）			財務省
	石油	ビジネス・エネルギー・産業戦略省			財務省
	ガス	共同管轄：ビジネス・エネルギー・産業戦略省と、ガス・電力市場局（Ofgem）[39]			財務省
運輸	航空	共同管轄：運輸省と、民間航空局（CAA）			
	鉄道	運輸省			財務省
	船舶	運輸省			
	道路	運輸省		スコットランドの閣僚	財務省
保健医療	医療環境	保健省	ウェールズの閣僚	スコットランドの閣僚	財務省
飲料水	飲料水	環境・食糧・農村地域省	ウェールズの閣僚	スコットランド飲料水水質規制当局	財務省
デジタルインフラ	デジタルインフラ	通信庁（Ofcom）			

[39] 特定の例外については、ビジネス・エネルギー・産業戦略省が唯一の所轄官庁である。詳しくは、「ネットワーク・情報システム規制 2018」のスケジュール1および2を参照のこと。

付録C：用語集

COBR — 内閣府ブリーフィングルーム。英国中央政府は緊急事態への対応においてCOBRを活用する。COBRは通常、ウェストミンスターにある物理的な場所であり、ここから中央の対応が始動、監視、調整される。政府対応の焦点として機能し、地方レベルの対応機関への助言において権威の源泉となる。

GCHQ — 政府通信本部。政府の信号情報活動およびサイバー国家技術局（NTA）の中心に立つ。

GFCE —「サイバー専門知識に関するグローバルフォーラム」

ICANN —「割り当てられた名前と数字のためのインターネット協力」（Internet Corporation for Assigned Names and Numbers）。ウェブサイト名とIPアドレスの調整を行う。

NATO — 北大西洋条約機構。

NCA — 国家犯罪対策庁

OECD — 経済協力開発機構。政府間の経済組織。

アクションフロード（Action Fraud） — 不正行為やサイバー犯罪の通報センター。イングランド、ウェールズ、北アイルランドの市民や組織が詐欺、詐取、サイバー犯罪に遭った場合、同センターにこれを通報する。スコットランドの場合、通報先はスコットランド警察である。

アクティブサイバーディフェンス（ACD） — 組織が脆弱性を発見・是正し、インシデントを管理し、サイバー攻撃阻止の自動化を進めることを支援する。一部のサービスは主に公共部門向けに設計されているが、その他のサービスは民間企業や市民も、適用可能性や実行可能性に応じて幅広く利用できる。

インシデント対応 — インシデントの短期的・直接的影響に対処する活動で、短期的な復旧を支援することもある。

インシデント管理 — システムやネットワークを損ねたり危害を加えたりする可能性のある有害なサイバー事象が現実的または潜在的に発生した場合に、それを調査して是正する活動を管理・調整すること。

インターネット — 様々な情報通信設備を提供するグローバルなコンピュータネットワーク。標準化された通信プロトコルを用いて相互に接続された多数のネットワークで構成される。

コネクテッドプレイス — 情報通信技術とIoTデバイスを統合してデータ収集・分析を行うコミュニティ。建造環境に新たなサービスを提供して市民の生活の質を高める。

サイバーインシデント — コンピュータ、インターネット接続機器、ネットワーク（またはこれらのシステムで処理、保存、伝送されるデータ）に対して現実的または潜在的に脅威となる出来事で、その結果を軽減するために対応措置が必要となるもの。

サイバーエコシステム — 相互接続されたインフラ、人、プロセス、データ、情報、通信技術、およびそれらの相互作用に影響を与える環境や条件の総体。

サイバーセキュリティ — インターネットに接続されたシステム（ハードウェア、ソフトウェア、関連インフラを含む）や、そこにあるデータ、およびそれらが提供するサービスを、不正アクセス、危害、不正利用から保護すること。ここには、システムの運用者が意図的に引き起こす危害や、セキュリティ手順の不順守または不順守へと巧みに誘導された結果として意図せずに引き起こす危害も含まれる。

サイバーセキュリティ・ボディオブナレッジ（CyBOK） — サイバーセキュリティを総合的に網羅する基礎的な知識体系。この種のものとしては初の独自リソースであり、サイバーセキュリティが広範な分野を包摂していることを示す。

サイバーリスク — ある特定のサイバー脅威が情報システムの脆弱性を突いて危害を引き起こす可能性。

サイバーレジリエンス — システム、組織、市民がサイバー事象に耐え、被害が発生した場合にはそこから回復するための総合的能力。

サイバー攻撃 —コンピュータシステムや、デジタル依存の高い企業、ネットワークを意図的に悪用して危害を与えること。

サイバー犯罪 — サイバーに依拠した犯罪（ICT機器の使用を通じてのみ成立する犯罪のうち、ICT機器が犯罪の道具であると同時に犯罪の対象でもあるもの）、または、サイバーを活用した犯罪（金融詐欺のようにICT機器を使用せずに行われる可能性もあるが、ICTの使用によって規模や範囲が大きく変わる犯罪）。

サイバー脅威 — 情報システムやインターネット接続機器（ハードウェア、ソフトウェア、関連インフラを含む）や、そこにあるデータ、およびそれらが提供するサービスに対し、主にサイバー的手段によって、そのセキュリティを侵害または危害を与える可能性があるもの。

サイバー評価フレームワーク（CAF） — 重要機能のサイバーリスクが、どの程度、担当組織によって管理されているかを評価する、体系的かつ包括的なアプローチを提供する。

セキュアバイデザイン（Secure by Design） — ソフトウェア、ハードウェア、システムに設計段階の最初からセキュリティが組み込まれていること。

デジタルツイン — 建造環境、社会環境、自然環境にある資産、プロセス、システム、制度の仮想的なレプリカまたは表現。複雑な物理的資産や市民がどのように行動するかについて洞察を与え、組織の意思決定の改善やプロセスの最適化に役立つ。現実世界の変化がツインに反映される一方、ツインの変化を現実世界に自動的に再現することが可能である。

デジタル規制のための計画 — 成長とイノベーションの促進を目的としてデジタル技術を管理するための、政府の全体的アプローチを規定する。

データ侵害 — ネットワーク上の情報を、当該情報へのアクセスや閲覧を許可されていない者に不正に移動または開示すること。

ドメイン — ドメイン名は、インターネット上の組織やその他のエンティティの場所を特定するもので、インターネットプロトコル（IP）アドレスに対応する。

ネットワーク・情報システム（NIS）規制2018 — 必要不可欠なサービスとデジタルサービスを提供するネットワークおよび情報システムについて、そのセキュリティレベル（サイバーレジリエンスと物理的耐性の両方）をレベルアップする法的措置となる英国の規制。

ファイブ・アイズ（Five Eyes） — 米国、英国、カナダ、オーストラリア、ニュージーランドの5カ国による情報（インテリジェンス）同盟の名称。自国民を脅威からできる限り安全に守るための情報共有を支援する。

ブロックチェーンテクノロジー — データ保存の特定の方法。ブロックチェーンは分散型台帳の一例であり、追記のみで改ざんができないストレージ技術の一種である。

ホライズン・スキャニング — 潜在的な脅威、リスク、新興課題および機会を特定するための体系的な情報調査。事態により良く備え、軽減と活用を政策決定プロセスに取り入れることを可能にする。

マイクロ生成 — 家庭、小事業者、コミュニティによる小規模なエネルギー生成。

マネージドサービスプロバイダー — 一連の定義されたサービスを顧客に提供し、それらのサービスの運営、維持、安全確保に責任を負う第三者。

モノのインターネット（IoT） — インターネット上で通信し、データを交換する電子装置、ソフトウェア、センサーを組み込んだ機器、車両、建造物、その他の製品の総体。

ランサムウェア — ユーザーのファイル、コンピュータ、デバイスへのアクセスを、身代金を支払うまで拒否する悪質なソフトウェア。

レガシーIT — ベンダーのサポート対象外か、または延長サポートやオーダーメイドサポートの対象になっているシステムおよびその構成ソフトウェアやハードウェアを指す。

人工知能（AI） — コンピューティングシステムが「自分で考える」ようにコード化され、自律的に適応・動作する技術。AIは現在、医療診断、創薬、予知保全等、より複雑なタスクでの活用が進んでいる。

国家サイバーセキュリティセンター（NCSC） — サイバー脅威に関する英国の技術的権威。サイバーインシデントの被害を最小限に抑えるための統一的国家対応を提供し、復旧支援や将来に備えた教訓活用を行う。

基幹サービス運営者 — 情報ネットワークに大きく依存する公共事業、医療、運輸、デジタルインフラ等の重要セクターの組織。ネットワーク・情報システム規制2018の基準で特定される。

完全性（Integrity） — 情報セキュリティ分野における完全性とは、情報が意図の有無に関わらず変更されておらず、正確かつ完全であることを意味する。

所轄官庁 —「ネットワーク・情報システム（NIS）規制 2018」に記載されている規制機関。NIS規制の対象となる様々なセクターに対して、様々な所轄官庁が存在する。

攻撃型サイバー（Offensive Cyber） — 物理的、仮想的、または認知的効果をもたらすために、システムやネットワーク上のデータを追加、削除または操作すること。攻撃型サイバーでは、技術的脆弱性を突いて、所有者や運営者が意図しない、または容認しない方法によってシステムやネットワークを使用することが多く、偽装や虚偽表示に依拠することもある。

政府サイバー調整センター（GCCC） — GSG、CDDO、NCSCの共同事業案。それぞれの機能と専門分野の結集を通じて、政府全体のサイバーセキュリティ運用努力の調整を改善し、政府全体でのサイバーセキュリティデータおよび脅威情報の利用方法を変革して、政府の「一体防衛」能力の真の強化を目指す。

暗号キー（Crypt-Key） — 英国政府が、政府、軍、国家安全保障関係機関にとって枢要となる重要情報およびサービスを、特に能力の高い敵対者からの攻撃対応も含めて保護することを目的に暗号を使用すること。

暗号技術 — コードや暗号を分析し解読する科学または学問。暗号解析。

暗号通貨 — デジタル通貨および決済システムの一つ。ビットコイン等。

産業用制御システム（ICS） — 製造、製品取扱い、生産、流通等の産業プロセスの制御や、インフラ資産の制御に使用される情報システム。

統合レビュー —「競争時代のグローバルブリテン：安全保障・防衛・開発・外交政策の統合レビュー」（Global Britain in a Competitive Age, the Integrated Review of Security, Defence, Development and Foreign Policy）。今後10年間の世界における英国の役割についての政府のビジョン、および、2025年までに政府がとる行動を説明。

脆弱性 — 攻撃者に悪用される可能性のあるソフトウェアプログラム内のバグ。

脆弱性報告サービス — セキュリティ上の欠陥が攻撃者に悪用される前に、組織に警告を発する仕組み。

自律システム — ルーティングが特定のエンティティまたはドメインの制御下にあるIPネットワークの集合体。

自治政府 — スコットランド、ウェールズ、北アイルランドへの地方分権により自治権を得たそれぞれの議会および行政府。地域内の政策課題に責任を負い、法律を制定する権限を持つ。

認証（Authentication） — ユーザー、プロセス、またはデバイスの IDやその他の属性を検証するプロセス。

運用技術（OT） — ハードウェアとソフトウェアを組み合わせて、特にエネルギー、製造、水、運輸等の産業セクターにおける物理的プロセスを監視、制御、自動化する。

重要国家インフラ — 損失や支障が出れば以下のような結果を招く、インフラの重要要素（すなわち資産、施設、システム、ネットワークまたはプロセス、およびそれらの運用・促進に必要不可欠な労働者を指す）。

a. 必要不可欠なサービスの可用性、完全性、提供に大規模な悪影響が及ぶ。ここには、完全性が損なわれれば多数の死傷者が出る恐れのあるサービスも含まれ、重大な経済的または社会的影響も考慮に入れる。

b. 国家安全保障、国防、国家機能に重大な影響が及ぶ。

量子テクノロジー — 量子物理学の原理を利用したテクノロジー。重ね合わせや絡み合わせ等のいわゆる「量子効果」の理解と制御が進めば、センシング、データ通信、暗号化、タイミング、コンピューティング等の経済社会を支える新たな技術革新の波が到来すると考えられている。