2012 年 11 月 28 日

サイバーセキュリティメモ 002

国際公共政策研究センター
主任研究員　石野　務

解説：英国「サイバーセキュリティ政策」

1. はじめに

インターネットの利用増加に伴い、英国でも、サイバー攻撃による国家安全保障への脅威が現実的なものとして認識されるようになった。英国政府は、2010 年に公表した“National Security Strategy”（国家安全保障政策）の中で、サイバーセキュリティを、国際的なテロリズムや軍事的危機、天災と並ぶ国家の最優先事項として位置付けた。

さらに、英国政府は、2011 年 11 月、“The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world”（英国サイバーセキュリティ政策：英国のデジタル世界を保護し進展させる）を公表し、サイバー攻撃に対抗して経済成長を促進し、国家安全保障や国民生活を守っていくことについて、国の方針を示した。本稿では、その概要を紹介する。

2. 概要

英国政府は、サイバー空間を、ビジネスをより効率的なものとし革新を生み出すものとして積極的に推進していく方針である。一方、サイバー空間の広がりとともにサイバー攻撃などのリスクも高まると認識し、サイバーセキュリティ強化の必要性を強く訴えている。

2011 年から 2015 年までの 4 年間において 650 百万ポンド（邦貨約 830 億円：@1 ポンド=128 円）のサイバーセキュリティ対策予算を確保し、情報局や国防省を中心にサイバーセキュリティ対策を推進して行く予定であり、国境を越えたサイバー攻撃などに対応するため、国際機関との提携や国際的な法的枠組みの整備を目指し、サイバーセキュリティ専門家の育成にも注力する。

サイバー脅威についての実業界や国民への通知も行っていく。また、「サイバーセキュリティハブ」や、「Get Safe Online」などを設置して、民間部門や国民と協働して脅威に対応していく。

(1)英国政府の目標

英国政府は、2015 年に向けて、サイバー空間がもたらす経済や社会の便益を確保するために、サイバーセキュリティに対する取り組みを改善していく方針であり、以下 4 つの目標を掲げている。

目標 1：

サイバー犯罪に立ち向かい、英国を、サイバー空間でビジネスを行う際に、世界で最も安全な場所の一つとする。

目標 2：

英国を、サイバー攻撃に対して、より回復力があるものとし、サイバー空間における英国の利益をより防御できるようにする。

目標 3：

開かれて安定した活発なサイバー空間の形成を助け、英国民が安全に利用できるようにし、開かれた社会を支持する。

目標 4：

英国の全てのサイバーセキュリティの目的を支えるために、分野横断的に知識や技術、能力を保有する。

また、これらの目標の実現において、以下 4 点を原則とすることとしている。

①リスクを前提としたアプローチ

②他国と見解を共有し協力する相互関係下での行動

③自由やプライバシーとセキュリティのバランス

④個人、民間企業、政府がそれぞれの役割を果たすこと

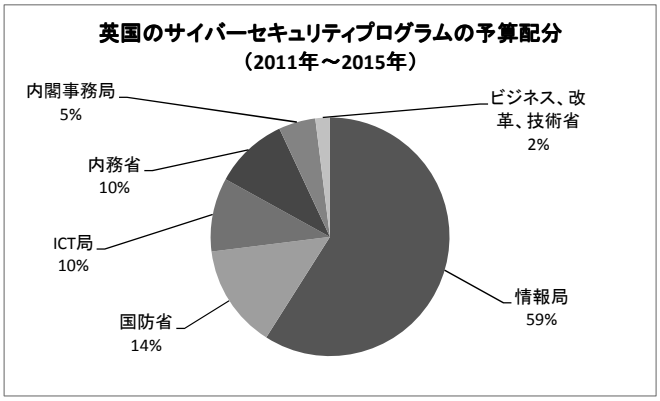
(2)体制・組織

情報局や国防省が、サイバー空間における英国の虚弱性や脅威の理解や低減の向上に大きな役割を果たしている。また、内務省や、内閣事務局、ビジネス・改革・技術省も、個別の特定の能力向上のために活動する。特に GCHQ（Government Communications Headquarters：政府通信本部）が、サイバー攻撃を検知し反撃する中心となっている。サイバーセキュリティに関する予算の半分がここに与えられる。

(3)予算

英国政府は、2010 年に、4 年間にわたる“National Cyber Security Programme”に対して 650 百万ポンドの予算を確保している。

本予算は、情報局や国防省を中心に、各省庁に対して配分される。



(4)国際連携

NATO の戦略的構想や、国家安全保障会議の決議に対応するために、英国は、サイバー脅威に対抗し、国の安全のために必要とされるサイバー環境の調査を行う。

英国はまた、国連や OSCE: Organization for Security and Cooperation in Europe において、事態の深刻化を軽減したり、サイバー空間での予期していなかったインシデントにより生じる国家間の誤解を防ぐために、実務的な信頼構築方法を発達させることを目的とした活動を活発に行う。

(5)国際的な法的枠組み

英国は、サイバー犯罪条約の広範な適用を行い、国境を越えた法の執行や、サイバー犯罪において安全な隠れ家がないことを示すために、柔軟な法の枠組みを整備する。

(6)教育・人材育成

専門家を維持し、英国のネットワークを良く防御することを可能とすることができる、善良なハッカーグループの育成を促進するために、英国は、以下を行う。

①2012 年 3 月までに認証専門家訓練のプログラムを設立し、情報の保護やサイバーセキュリティの専門家の技術水準を引き上げる。

②専門家に新たな才能を採り入れるために「Cyber Security Challenge」の助成を継続する。

③サイバーについての深い知識を有する専門家を増やすために、大学院の教育を強化する。

④サイバーについての分野を横断した調査を発展させ、英国の学術的な基礎を強化する。

⑤GCHC の援助を得て、3 年半、2 百万ポンドの予算で、サイバーセキュリティについての調査機関を設立する。

⑥民間部門におけるサイバーセキュリティについての要求の範囲、パターン、性質に関する調査を委託する。

(7)その他サイバーセキュリティに関する政策

英国は、サイバーセキュリティの強化のため、以下の政策も実施する。

ⅰ.「サイバーセキュリティハブ」の構築

民間部門と政府は、①サイバー脅威や、インシデントへの対応強化に関する情報を交換すること、②新たな傾向を分析し、新たに発生する脅威や可能性を識別すること、③英国の総合的なサイバーセキュリティ能力を強化し連携させること、に焦点を当てた革新的な新しい取り組みを企画する。

そのために、政府や民間における脅威についての情報を収集し、重要な産業の「NODE：結節点」にその情報を伝え、どのようなことをすべきかを識別することを助け、成功事例を分かち合う体制として、「サイバーセキュリティハブ」を構築する。これについては、2011年12月から、防衛、金融、通信、医薬、エネルギーの5つの分野で、試験的なものを始める。

ⅱ.「Get Safe Online」の開始

オンラインセキュリティに対する関心を向上させるための官民の共同キャンペーンとして、一般の国民や小規模企業を対象とした「Get Safe Online」を開始する。

これは、様々なコミュニティグループと活動を行い、国民にインターネットを安全に利用するノウハウや信頼を与えることを目的としたものである。ウェブサイトでマーケティングやPR活動を行い、最新の助言や道具、成功事例についてのガイダンスを与えたり、オンラインショッピングや、データの窃盗、身元の詐称などについての助言を行う。

3. 英国サイバーセキュリティ政策の特徴について

英国は、サイバー空間を、ビジネスをより効率的なものとし、より低いコストで購入を行えるようにすることにより世界を成長させるものとして積極的に評価している。一方、サイバー空間が経済や社会においてより中心的な存在になり役割が増すにつれて、その虚弱性を利用したサイバー攻撃による脅威も多くなると警戒している。

サイバーセキュリティ対策においては、①全てのネットワークシステムは潜在的に虚弱であると認識し、リスクを前提としてアプローチをとること、②脅威に対抗するための専門知識や革新はビジネス主導となることや、インターネットの無国籍性を考慮し、相互関係の下で活動すること、③英国民のプライバシーの権利やその他の自由に関する基本的権利を保護しながら個人や社会全体の安全性を高めることも目指し、自由やプライバシーとセキュリティのバランスを取ること、の3つを基本原則に挙げている。ここでは、民間企業や国際的な共同の必要性や、国民の基本的人権への配慮の必要性を強調しており、英国をサイバー空間における国際的先進国とするために、国際的な連携や、民間部門との連携

も重要視している。また、個人、民間部門、政府がそれぞれサイバーセキュリティにおいて重要な役割を負っており、ともに行動することが必要と訴えている。

サイバーセキュリティのために、4 年間で 650 百万ポンド（邦貨約 830 億円：@1 ポンド=128 円）の予算を確保し、情報局、国防省を中心とした関係部署に割り振り、①政府や民間の脅威についての情報収集、情報伝達などを目的とした「サイバーセキュリティハブ」の設置や、②サイバーセキュリティ専門家集団の育成、③サイバー犯罪に関する法律の強化、④国民への周知、⑤実業界の認識の向上、⑥サイバーセキュリティ部門のビジネスの機会の増加、などの具体的な政策を掲げている。

4.　抄訳（本文より抜粋して翻訳）

■英国サイバーセキュリティ政策
―英国のデジタル世界を保護し進展させる―

1. サイバー空間：英国や世界を成長させ強化するもの

インターネットやデジタル技術は、経済成長を加速し、人々に新たな交流手段を与えることにより社会を変化させてきた。インターネットは、我々の生活に根本的な変化をもたらした。インターネットが発達した先進国では、この 15 年間に一人当たりの実質 GDP が 500 ポンド増加したが、同様の効果を工業の改革で得るためには、50 年間が必要であった。

サイバー空間は、ビジネスをより効率的なものとし、購入をより低いコストで行うことを可能とする。英国はサイバー空間を積極的に活用してきた。2009 年には 6 億 8 百万件のカード支払いがオンラインで行われ、その支払い総額は 472 億ポンドにのぼった。2011 年には、英国の 74%の家庭がブロードバンドにアクセスした。(2010 年の欧州の平均は 60.8%)

最近の調査では、インターネットは、新興国において GDP の 3.4%に貢献し、英国では GDP の 6%に貢献していると報告されている。これは、公共インフラサービス（ガス、電気、水道）や農業よりも大きい貢献である。

サイバー空間は、インフラの自動化や最適化にも貢献している。例えば SCADA システム[1]は、工業や、水の供給、精製、発電などの製造過程を自動的に制御することができる。また、電話や直接の対話の代わりに E-Mail を使うことで費用の削減が行える。共通の情報通信技術インフラを導入することにより、2014、2015 年に、政府は 460 百万ポンドの費用削減を行うことが可能となろう。

世界中の多くの人がサイバー空間に参加することにより、新しい予想もされなかった使い方が生まれ、より便利になる。クラウド・コンピューティングや、スマートグリッドの導入、モバイルによる作業の増加、サイバー空間の利用者の増加など、変化のペースは留まるところがない。サイバー空間は、英国や世界の国々にとって、より価値があり重要なものとなっている。

2. 変化する脅威

インターネットは、我々の経済や社会において、急速に中心的な存在になっている。サイバー空間の役割が重要になるにつれて、新たな機会と同時に新たな脅威が生まれている。

我々が依存しているデジタル構造物は、効率性と相互運用のために作られている。最初にインターネットが作られた時には、安全性についてはあまり考慮されていなかった。だ

[1] Supervisory Control And Data Acquisition の略。産業制御システムの一種で、生産工程やインフラ設備をコンピューターによって監視し、プロセス制御を行う。地理的に分散したシステム群を遠方監視制御装置などにより集中監視制御する。

が、我々がそれに依存するようになるにつれて、問題が大きくなった。人々は、国家の安全や、経済の繁栄、個人の生活を支えるインターネットが、安全で回復力のあることを望んでいる。

残念なことに、サイバー空間を利用して盗みを行ったり、重要なデータを破壊しようとする敵対者の数は増加している。我々の依存が大きくなっているため、我々の財産や、重要なインフラや、仕事場や、家庭など全てが影響を受ける可能性がある。2010 年の国家安全戦略では、英国におけるサイバーアタックを、対抗について最も高い優先度を有する「第一段階の脅威」と定めている。

“脅威とは何か“

英国を攻撃目標とした、世界中から行われる様々な方法の犯罪が、すでにインターネットで認識されている。特にコンピューターのネットワークや、オンラインサービスを目標とした犯罪は、デジタルの世界でしか存在しないものである。サイバー空間は、英国を標的とした犯罪を世界中から行うことを可能とし、法の適用を困難にしている。ビジネスや公共サービスの仕事がオンラインで行われることが増えるにしたがって、潜在的な標的は多くなる。

サイバー空間における英国に対する最も洗練された脅威には、ほかの国から来るものがある。これは、我々の政府や軍隊や産業の経済的な財産をスパイしたり、情報を盗むことを目的としている。愛国者的なハッカーは、国家に代わって誤情報を流したり、重要なサービスの提供を妨害する。戦争時には、サイバー空間の脆弱性が敵に利用されて、軍隊の技術的な優位性が減少したり、重要なインフラ設備が攻撃される。

サイバー空間は、すでにテロリストによって、プロパガンダを広めたり、潜在的な支持者を活性化させたり、資金を集めたり、連絡を行うために利用されている。テロリストが物理的な攻撃を行おうとする一方で、サイバー空間を英国に対する攻撃に用いる可能性が増している。我々は、テロリストが英国のインフラが脆弱であると考えているのであれば、この状態は続くと判断している。

英国に対する政治的な動機を有した活動家からの脅威も現実に存在している。活動家による公共や民間部門のウェブサイトへの攻撃は、ますます増えている。

犯罪者、テロリスト、外国の間諜や軍隊などからの英国に対する攻撃は活発化している。しかし、国境がなく、匿名性があるというインターネットの特性により、正確な特定は困難であり、敵対者の認識がますますできなくなっている。

“ビジネスへの影響”

組織は、サイバー空間への依存がもたらす新たな脆弱性をいつでも認識しているわけでない。知的財産やそのほかの商業的に重要な情報（ビジネス戦略など）は、魅力的な攻撃対象となりうる。2011 年に、ソニーはプレイステーションのネットワークを攻撃され、1

億人の利用者の情報が漏えいした。ネットワークは数週間封鎖され、ソニーの損害は 171 百万ポンドと推定された。

個人と組織間のデジタルによるつながりの増加に伴い、攻撃が、より多くの個人や組織に影響を与えるようになっている。最近の調査では、毎年の英国のサイバー犯罪による損害は 270 億ポンドにのぼると報告されている。サイバー犯罪は、スマートフォンのような新たなサービスに対しても迅速に対応できる。

サイバー空間で安全を保つことは、複雑で困難で費用がかかる。脅威や脆弱性の性質や大きさについての明瞭な認識が無ければ、防御や防止に対する投資は無駄に終わる。

“我々のセキュリティに対する影響”

サイバー空間の利用の増大は、その途絶が、危機における国家の効率的運用に影響を及ぼすことを意味している。毎月 2 万件を超える悪意のあるメールが政府のネットワークに表れる。そのうち 1,000 件は、政府をターゲットとしたものである。既存の防衛やセキュリティと共に、英国は、サイバー空間における国家の利益も防衛できなければならない。

“個人や社会への影響”

インターネットを最大に活用するためには、個人がそれを安全に使えることに信頼性を感じていることが重要である。我々が仕事や個人の生活においてインターネットを使うようになればなるほど、それは、犯罪者にとって魅力的な標的となる。

個人への影響以外に、サイバー空間が広く用いられるようになり、社会に対してより広く影響を及ぼすようになっている。英国では伝統的に、自由や、正義、透明性や法治などの中核的な価値に導かれる方法で国民の権利が守られてきた。これらの価値が、我々を、我々は何者であるのか、我々は何をすべきか、そして英国民でいることは何を意味するのかを明確化することを助けてきた。相互接続したサイバー空間の性質やその拡大が、これらの価値の推進を発展させてきたと考えられる。

サイバー空間で行われる行為にかかる取決めや規範は、まだ開発中である。我々の国家の安全性の強化において、表現の自由や、アイディアを探し受容し取り入れる権利、プライバシーの権利を考慮する必要がある。他の伝達手段と同様、サイバー空間で自由を制限する可能性もある。すでに、サイバー空間における統制や制限について検討を行っている国家や組織もある。英国は、世界の善意の国々と協力し、サイバー空間がもたらす便宜をフルに活用できるように働きかけていく。

“複雑な課題”

インターネットやデジタル技術の導入は、急速な動きや複雑な環境を生み出し、新たな課題をもたらす。

サイバー空間は、多くが商業的に保有され国際的であるという性質を有している。

サイバー空間を形成するシステムは、国際的で多様な供給者による構成物から作られている。数多くの下請け製造者がこれを生産し、テストし、部品を組み立てている。

イベントが起きるペースが早く、既存の防御や対応では追い付かない。サイバー空間の複雑性と共に、これが敵対的な行動の特定を困難にする。また、脅威が潜在的であることから、公共や民間企業がそのリスクを過小評価しやすい。

“問題に対応する既存の能力”

英国の民間部門、政府の主要な官庁、学会は、サイバー空間における国際的に先進であることの強みを有している。

英国は国際的な連携を有している。英国は、すでに民間部門とサイバー空間から発生するリスクについての情報交換を行い、サイバー犯罪に対して協力して立ち向かっている。GCHQ（政府通信本部）は、国際的に優れた技術を保有している。だが、政府の能力は、デジタル時代の拡大するセキュリティの課題に対応するのに十分ではない。インフラを運営している組織に対して、政府は助言を与えているが、これは、より拡大される必要がある。

実業界では、リスクの大きさを認識している会社もあるが、特に中小企業には、自分を防御するのに十分な技術や知識を有していない会社もある。

国民が、脅威を理解し適切な行動をとることができるように、情報や必要な技術にアクセスできることが必要である。政府は民間部門の協力を得て情報伝達を強化する必要がある。

サイバー空間が世界を変えていることは明らかである。それは莫大な便宜をもたらす一方で、新たな虚弱性も生じさせる。リスクは、動的で変化する性質を有しており、新たな取り組みを必要としている。

3. 2015 年に向けた英国のサイバーセキュリティの構想

サイバー空間がもたらす経済や社会の便益を確保するために、我々はサイバーセキュリティに対する取り組みを改善していく。

(1)我々の構想

我々の構想は、2015 年に、我々が、活発で回復力がある安全なサイバー空間から、経済的、社会的な価値を引き出すことである。サイバー空間で、我々は、自由、公正、透明性、法律による統治などの我々の中核的な価値に導かれて、国家の安全や、強い社会や、繁栄を高める活動を行う。

(2)我々の目標

目標１：

サイバー犯罪に立ち向かい、英国を、サイバー空間でビジネスを行う場合に、世界で最も安全な場所の一つとする。

目標２：

英国をサイバー攻撃に対してより回復力があるものとし、サイバー空間における我々の利益をより防御できるようにする。

目標３：

開かれて安定した活発なサイバー空間の形成を助け、英国民が安全に利用できるようにし、開かれた社会を支持する。

目標４：

我々の全てのサイバーセキュリティの目的を支持するために、分野横断的な知識や技術、能力を保有する。

(3)我々の原則

“リスクを前提としたアプローチ”

サイバーアタックの検出が困難で、すべてのネットワークシステムが潜在的に虚弱である国際的な世界において、完璧な安全はあり得ない。そこで、我々はリスクを前提としたアプローチを行う。

“相互関係の下に活動する”

問題の大きさから強力な国のリーダーシップが必要とされる。政府が単独で行動することはできない。我々が守るべきインフラの多くは民間に所有され運営されている。脅威に対応するための専門知識や革新は、ビジネス主導となる。

我々が国内の防衛を強化できたしたとしても、インターネットは基本的に無国籍である。我々が依存しているすべてのインフラが英国内にベースを持っているわけではない。我々は他国と見解を共有し、協力しなければならない。

“自由やプライバシーとセキュリティのバランス”

国内では、我々は、英国民のプライバシーの権利やそのほかの自由に関する基本的権利を保護しながら、個人や社会全体の安全性を高めるサイバーセキュリティ政策を追求していく。国際的には、英国はサイバー空間で許容できる活動についての基準の展開を追求していく。

(4)役割と責任

これらの目標の実現のために、民間部門、個人、政府すべてがともに行動しなければならない。

“個人”

普通の人々は、サイバー空間を、商売を行ったり、生活を行う安全な場とするために重要な役割を負っている。2015 年までに、我々は英国を以下のようにしたい。

①人々が、基本的な水準のオンラインの脅威に対する防御を知っている。人々は、オンラインの脅威に関する適切かつ最新の情報や、自信を防御するための技術や実務にアクセスできる。

②インターネットに個人情報や重要な情報を掲載することに注意深く、発信不明者からのメールの添付物を警戒し、ウェブサイトからのファイルのドローダウンに慎重になっている。

③家や仕事場にいるものが誰でも、サイバー空間の脅威を認識し、それを報告することができる。

④個人が、パスワードを保護したり、ソフトウェアやオペレーティングシステムを定期的に更新することコンピューターや、第三者に利用されて脅威を増大させることを防ぐために対応プログラムを働かせることの重要性を理解することにより、会社や政府の安全性を守ることができる。

⑤オンラインの世界では、我々がここにサイバー空間における行動に責任を負っていることを、人々が良く理解している。

“民間部門”

民間部門は英国のサイバーセキュリティにおいて重要な役割を負っている。サイバー空間の大部分は民間の会社によって所有され運営されている。セキュリティの課題に対応するために必要な革新は実業界によって行われる。2015 年までに、我々は英国を以下のようにしたい。

①企業が脅威を認識し、商業上重要な情報や知的財産権や顧客データを保護しながらサイバー空間を利用する。

②民間企業が、他社や、政府、警察などと、共通の脅威への対応を改革しサイバー空間で直面する脅威を防止するために、情報や資源を共有して、協働する。

③民間部門が、サイバーセキュリティに関する英国の技術を強化し、将来我々が必要とするサイバーセキュリティの技術を供給する先進技術のセンターを創立する。

“政府”

2015 年までに英国は以下を行う。

①最も強力な脅威を認識し打ち破る能力を構築する。

②サイバー空間における「新たな規範」についての国際的な同意形成を助成する。

③政府のシステムや国の重要なインフラの虚弱性を減少させる。

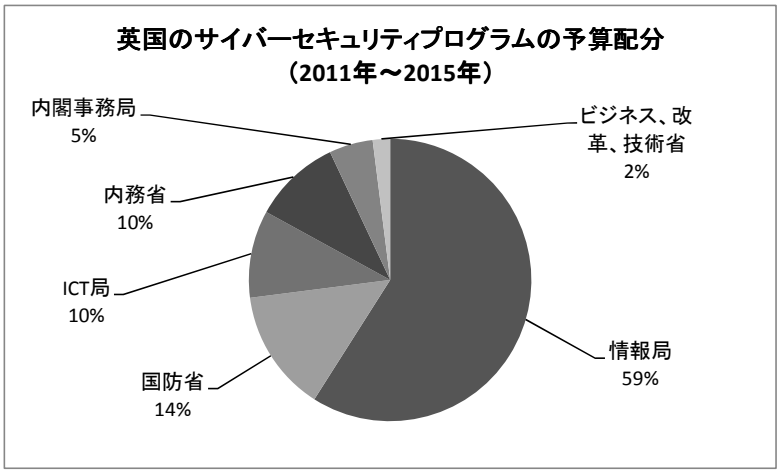
④サイバーセキュリティの専門家の幹部を育成する。

⑤法の強制力を強化して、サイバー犯罪に対抗する。
⑥予防や国民の認識を高める。
⑦実業界における認識を高める。
⑧実業界や学会と連携してサイバーセキュリティ市場における英国のシェアを高め、英国をビジネスオンラインを行う際に、安全な場所であるという地位を固める。

4. 行動:脅威に対応し、機会を捉える

英国政府は、2010 年に、4 年間にわたる“National Cyber Security Programme”に対して 650 百万ポンドの予算を確保した。

情報局や国防省が、サイバー空間における英国の虚弱性や脅威についての理解や、その低減の向上に大きな役割を果たしている。内務省や、内閣事務局、ビジネス・改革・技術省も、個別の特定の能力向上のために予算を用いる。



“行動の優先順位”

我々は、以下によって英国の既存の強みを強化していく。

①特に英国のインフラや国益に関連するシステムに焦点を当てて、高度なサイバー脅威の検出と分析を強化していく。国家的な本物の対応を構築するために実業界のパートナーと共に、知識や状況認識を蓄積する。
②高性能の、国家が背景にある脅威を防止する能力を高め、それらの技術が非国家的な活動家の手に渡ることを防ぐ。
③サイバー空間の活動に対する「交通規則」や、国際的な原則を発展させるために国際的な活動を行う。他の諸国と実務的な信頼構築の方法で、リスクの深刻化を減らし誤解を防ぐために協力する。
④サイバー犯罪条約を批准したが、互換性のある法律の発展のために他国を説得し、サイバー犯罪が国境を越えても訴追できるようにする。

⑤国内では、我々は効果的な法的体制を保ち、サイバー犯罪に対して対抗し訴追できる強制力を保持できるようにする。サイバー犯罪について報告を行いやすくし、報告を受けた情報局がそれを効果的な対抗措置につなげたり、国民に助言を行うことを確実にする。また、場合によっては、オンラインでの脅しやインターネットでの詐欺のようなサイバー犯罪に対抗するために、サイバー関連の制裁を行う。

⑥我々は、政府自身のシステムにおけるサイバーセキュリティの成功事例をモデル化し、政府に対する供給者に対して高い水準を要求することにより、基準のレベルを上げる。

⑦我々は、英国がこの分野で優位性を保ち、革新的な解決策を創造し続けることができるように、基礎的な調査や開発を行う、サイバーセキュリティの技能のある専門家の幹部を育成する。

⑧予防が重要であり、我々は、国民や民間会社がオンラインで自分自身を防御できるように、注意を喚起し教育を行う。最近の攻撃の 80%以上が、定期的に対抗ソフトを更新するなどの成功事例を追随することにより、防ぐことができた。

⑨我々は、英国が海外のビジネスを得て成長に貢献するような、サイバーセキュリティ製品やサービスの活発な市場を創造する。それは、また、英国をサイバー空間でビジネスを行うのにふさわしい場所とすることを可能とする。

“質の高い脅威に対抗し防止する能力を創造する”

・2010 年の NATO リスボンサミットでは、サイバー分野は、同盟国にとって顕著に新たなリスクと可能性をもたらすものとして位置付けられた。同盟国に示された新たな戦略的な構想は以下の通りである。

「サイバー攻撃を予防し、防止し、防御し、攻撃から回復する能力を発展させる。それには、NATO の国際的なサイバー防御の能力を高める計画を用いたり、統合させることや、全ての NATO の部署を集中化されたサイバー防御の下に置いたり、NATO 参加国間のサイバー攻撃に対する認識や警告、対応を見直していくことなどが含まれる。」

・NATO の戦略的構想や、国家安全保障会議の決議に対応するために、NCSP は、サイバー脅威に対抗し、我が国の安全のために必要とするサイバー環境の調査を行う。そのために、我々は、より先を見越した取り組みを行うための投資を行っている。

・国防省では、軍事的なネットワークや軍備がサイバー攻撃から防御されていることを認識するための投資がすでに行われている。2012 年の 4 月から、サイバーの防御能力の向上のために、新たな総合部隊が任務に就いている。

・この一環として、我々は、防衛からサイバー能力を引き出すことを目的として、新たな防衛サイバー作戦グループを編成した。

・国防省は、最近、Corsham に、武力のサイバー防御に焦点を絞って活動する、Global Operation and Security Control Centre を設立した。また、Corsham のセンターに、Joint Cyber Unit を設け、我々の情報セキュリティに対する脅威に対抗する積極的な方法を含

む、新たな技術を開発し、活用することとする。
・国防省は、サイバー脅威に対する認識や、対応、虚弱性、事例についての蓄積を向上させるために、主な同盟先や産業との関係を強化する。
・650 百万ポンドの予算の約半分は、英国の主要な能力の向上に用いられる。これは、主として Cheltenham の GCHQ（政府通信本部）に与えられ、サイバー攻撃を検知し反撃することに用いられる。

“サイバー空間における役割の分担についての国際的同意を構築するための活動”

・同時に、我々は、サイバー空間での行動の「交通ルール」についての国際的な基準を発展させるために活動する。
・手始めに、英国は、全ての政府が、サイバー空間において、国内法や国際法に則り、均整に行動すべきであると考える。これには、知的財産や表現の自由や集会の自由などの基本的人権の尊重も含まれる。
・英国は、2011 年 11 月にロンドンにおいてサイバー空間の会合を主催した。英国はまた、国連や Organization for Security and Cooperation in Europe（OSCE）において、事態の深刻化を軽減したり、サイバー空間での予期していなかったインシデントにより生じる国家間の誤解を防ぐために、実務的な信頼構築方法を発達させることを目的として活発に活動している。

“政府のシステムや、重要なインフラの虚弱性の軽減”

・政府の ICT 戦略は、「政府がいかにその重要な情報やシステムを防御し回復させていくか」ということから始まる。我々は産業界と共に、政府やその公共サービスネットワークに供給される ICT 製品やサービスのために、堅固なサイバーセキュリティや IA 基準を開発する。特に、我々は、重要な防衛装備の供給者に対するサイバーセキュリティの水準を引き上げる予定である。我々が、供給者に対する物理的なセキュリティの水準に対する要求を定めたように、サイバーセキュリティを通したデータの盗用の可能性があるだけに、サイバーセキュリティの水準についても見直すべきである。国防省は、ICT 戦略を通して、リスク管理の統治を強化し、情報保護の管理において政府がすでに構築したことを発展させることにより、政府の情報に関するリスクを管理する取り組みを主導している。
・英国は近々、政府の「何もなければデジタルで」計画に則り、公共サービスのオンライン化の大掛かりな拡張を行う予定である。これらの多くのサービスは、現在準備中のクラウドサービスに移行される予定である。政府は、最近、「クラウドコンピューター戦略」を公表し、この移行がいかにセキュリティを侵害せずに実行されるかを説明した。顧客に対するサービス供給や効率を向上させることは正しいことであるが、我々は、そのサービスが安全で、詐欺やサイバーアタックに対して回復力があることを確認しなければ

ならない。政府は、政府のサービスを供給するのに用いられる多くの技術プラットフォームを確認している。これは防御を向上させ、防御的な監視の強化ができる。サービスの利用者を識別し、詐欺を防ぐために、NCSP は、身元保証やその他の補助方法のために、信頼がおけて回復力のある接近方法に関する研究に、資金を拠出している。

・実際には、英国の重要なインフラ設備の大部分は、政府ではなく民間セクターによって所有され運営されている。Centre for the Protection of National Infrastructure（CPNI）は、すでに国の重要なインフラ設備会社と協働して、重要なシステムやデータを防御するために必要な手段をとろうとしている。

・CPNI は、テロや、サイバー空間からのものも含めたスパイなどその他の脅威に対する国のインフラ設備機構の脆弱性を減少させる目的で、助言している。本機構はすでに、国のインフラに関する民間部門の機構と強い協力関係を築き、相互の利益のために、情報交換を行える環境を整えた。他の省庁の部署や専門的なサービス機関などを含むネットワークを拡充することにより、直接的な関係が増強されている。

・政府は、このアプローチを、現在対象としている重要なインフラ関連の企業ばかりでなく、企業収入や知的財産に対する行為が英国の経済に損害を与える可能性のある企業グループにまで拡げようとしている。

・これらの広範囲にわたるグループが、脅威や、脅威に対抗するために何が行えるかについての実施可能な情報を入手できるように、サイバーセキュリティの「ハブ」が設立される予定である。

＊「サイバーセキュリティハブ」について

2011 年 2 月、英国首相は、英国経済の各分野のトップ企業の首脳と面談し、サイバー脅威に適切な対応を行うことについての共通の利益について話し合った。それから 1 か月後、民間部門と政府は、以下に焦点を当てた革新的な新しい取り組みを企画し構築することとなった。

①サイバー脅威や、事故に対する対応強化に関する情報を交換すること
②新たな傾向を分析し、新たに発生する脅威や可能性を識別すること
③我々の総合的なサイバーセキュリティ能力を強化し、連携させること

公共と民間部門の共同の「ハブ」は、政府や民間の脅威についての情報を収集し、重要な産業の「NODE：結節点」にその情報を伝え、どのようなことをすべきかを識別することを助け、成功事例を分かち合う体制を構築する。2011 年 12 月から、防衛、金融、通信、医薬、エネルギーの 5 つの分野で、試験的なものを始める。これから得られた教訓は、2012 年 3 月から開始される他の分野への拡大のために用いられる。我々は、中小企業も脅威を認識し、「サイバーセキュリティハブ」から利益を得ることができるような方法を構築する予定である。

“サイバーセキュリティ専門家集団の育成”

・技術変革のペースは過酷である。遅れをとらないためには、サイバー空間やそれがどのように進化するかについて深い知識を有している人を必要とする。ただし、そのような人は政府や実業界には稀にしかいない。民間部門のサイバーセキュリティの技術と専門知識への要求が増大し、実業界や教育や訓練を行う者がそれに対応しなければならなくなると警告する声が上がっている。要求の高まりに応え、英国の専門家を維持し、我々のネットワークが良く防御されていることを助けることができる善良なハッカーグループの発展を促進するために、NCSP は以下を行う。

①2012 年 3 月までに認証専門家訓練のプログラムを設立し、情報の保護やサイバーセキュリティの専門家の技術水準を引き上げる。

②専門家に新たな才能を採り入れるために「Cyber Security Challenge」の助成を継続する。

③サイバーについての深い知識を有する専門家を増やすために、大学院の教育を強化する。

④サイバーについての分野を横断した調査を発展させ、英国の学術的な基礎を強化する。

⑤GCHC の援助を得て、3 年半、2 百万ポンドの予算で、サイバーセキュリティについての調査機関を設立する。

⑥民間部門におけるサイバーセキュリティについての要求の範囲、パターン、性質に関する調査を委託する。

＊Cyber Security Challenge：郵便配達人からサイバー専門家に

英国は、技術的な技能と、問題解決や調査への適性を有したサイバーセキュリティの専門家を必要とする。Cyber Security Challenge は、才能のある個人を選別するための多様な参加者を迎える挑戦的な試験を行う。最近の合格者は、郵便配達人として働いていたが、今では英国郵便のためのセキュリティの専門家として働いている者もある。

“サイバー犯罪と法律の強化”

・我々は、警察がサイバー犯罪に対抗できるように、英国が強力な法律の枠組みを有していることを保証する。

・サイバー空間では犯罪者が世界中から犯罪を行うことを可能とするので、我々はサイバー犯罪条約の広範な適用を行い、国境を越えた法の執行や、サイバー犯罪に対する安全な隠れ家がないことを示すために、柔軟な法の枠組みを整備する。

・適切な法律の制定が行われていることが不可欠であるが、要求された場合に実施できる合意が必要である。我々は、ネットワーク世界のリアリティを反映させるために早いペ

ースで実施される、実務上の協働や、国境を越えた法の執行能力の育成を必要とする。英国は、法の執行のネットワークの接続先としての「24/7 Network」の強力なサポーターである。これは緊急な援助が必要とされる場合に、パートナー国がそれを得ることができる最善の方法である。Serious Organized Crime Agency がすでに世界中に連絡事務所を有している。

・我々はまた、英国内でも協力に対応できることを確実にする必要がある。国内では、我々は、迅速な技術面の変更が行われる分野における目的に、それが合致しているかどうかについて、英国自身の「Computer Misuse Act」の見直しを行っている。改定が必要とされる場合にはできるだけ早くそれに関する提案が行われる。

・政府はまた、何者かがより深刻なサイバー犯罪攻撃を行うと信じるに足る強い理由がある場合には、国民を守るために裁判所がすでに追加的な権限を保有していることを、警察や裁判官に知らしめる必要がある。犯罪者が釈放された場合や、「重要犯罪防止指令」（2007 年　重要犯罪令）が出された場合などに、コンピューターの使用が監視されたり、許可証の条件によって制限されうる。例えばコンピューター詐欺を行った者に対して、オンラインによる販売が制限されうる。

・さらに、法務省や内務省は、サイバータグを用いた制限を考えている。これは、犯罪者がインターネットに付された条件を破った場合に、自動的に警察や保護観察官に通知を行うしくみである。

・現在、警察が保有している権限を拡げる一方で、我々は運用上の対応も強化している。National Crime Agency（NCA）の設立の一環として、我々は、SORA の e-crime ユニットや、都市警察の e-crime ユニットで現在行われている機能をまとめて、新たな国際的なサイバー犯罪機能を設立する。このユニットは、最も深刻な国レベルのサイバー犯罪を取扱い、国の重大な事故の担当となる。NCA は、英国内の警察のサポートも行う。

・我々が現在、警察と実業界と地域社会の連携を強めようとしているが、そのためにそれぞれの業界間の技術の伝達を推奨している。

・電子売買や、ビジネスのあらゆる要素を支えるネットワーク技術の増大は、犯罪者にとって魅力的な標的が増えていることを意味する。これらの犯罪への対抗に関しては、特に実業界が重要な役割を果たす。我々は、子供に対する脅威に対抗するために産業界や、警察、そして政府を、UK Council for Child Internet Safety（UKCCIS）に呼び込むことによって成功を収めた。我々は、首相の呼びかけの下、サイバー犯罪における「セクターを超えた仕事」を発展させるために、様々な分野にグループを集める類似のフォーラムを開催する予定である。このフォーラムは、犯罪対策オンラインをデザインし、セキュリティにおける成功事例や、産業界の全てのレベルに効果的な犯罪防止策を助言することを発展させることに役立つ。

・並行して、国民にサイバー犯罪を報告することが、単純で簡単なことであることを知らしめるための行動を開始する。過半の警察署は、すでにオンラインによる国民からのサ

イバー犯罪報告を受ける装置を備えている。

“予防と国民への周知”

・予防が重要である。一般的なサイバー犯罪は非常に単純な「サイバーウィルス予防策」によって防ぐことが可能である。GCHQ は、最近成功されたサイバーアタックの 80%以上は、簡単な成功事例、例えばアンチビールスソフトウェアを定期的に更新することによって防止できたと推定している。

・国民が自分自身を保護できるように、我々は以下を行う。

①社会的なメディアを用いて、詐欺や他のオンライン脅威について警告し、「新たに普及している脅威」に消費者が対応することを助ける。

②国民が、サイバー空間を安全に利用できるように、全ての層に対するサイバーセキュリティ教育を強化する最良の方策を考える。

③インターネット会社と協働して、オンライン攻撃に対するオンライン制裁の可能性を調査する。

④インターネットサービスプロバイダーと協働して、個人が所有のコンピューターから情報漏えいがなかったかを確認したり、あった場合に何をすべきか、あるいは将来の攻撃に対してどうやって自分を守るのかを確認することを助ける。

⑤明確な「サイバーセキュリティ助言」を提供して、国民がどのようにコンピューターを使用したらよいのかを教えたり、リスクを伝える。

⑥セキュリティについての「カイトマーク（英国規格協会の認証)」の発展を促し、セキュリティ製品を購入する国民に対する情報を強化する。BIS は、国内や、欧州、あるいは国際的な品質機関と協働して、消費者が、市場を探る際に、サイバーセキュリティについての適切な水準を有する会社や、良いサイバーセキュリティ製品を識別化できるように、工業製品の水準やガイダンスを発展させる。

・「Get Safe Online」が、すでにこのような努力が行われる場として存在している。我々は、投資家や、インターネット会社、小売業者、インターネットプロバイダーなどと、これらをどのようにして向上させて相互作用的なものとするのか、より持続可能な活動とするにはどうしたらよいのか、国民に追加的なサポートの発信源をどのように知らせるのか、どうやって「カイトマーク」を用いて消費者が本当に助けになる製品を見極めさせるのか、などについて話し合った。

＊「Get Safe Online」について

「Get Safe Online」は、オンラインセキュリティに対する関心を向上させるための官民の共同キャンペーンで、一般の国民や小規模企業を対象としている。様々なコミュニティグループと活動を行い、国民にインターネットを安全に利用するノウハウや信頼を与えることを目的とする。また、様々なウェブサイトでマーケティングや

PR 活動を行い、最新の助言や道具、成功事例についてのガイダンスを与える。オンラインショッピングや、ソーシャルネットワーク、データの窃盗、身元の詐称などについての助言も含まれる。

“実業界の認識を高める”

・消費者との協働と同様、我々は、サイバーアタックによる、評判や、収入、知的財産への潜在的脅威についての実業界における認識を高める必要がある。

・実業界が、サイバー空間で実行される犯罪や経済的なスパイ活動の最たる犠牲者になる。問題に関する責任は、政府と民間部門の間で分担されるべきである。究極的には、資産を保有し、より進んだサイバーセキュリティを導入するかについての実務上の決断を行うのは民間部門である。我々は、すでに、サイバー脅威や、実業界が自身の資産を守るために何を行うべきかについて、認識を高めるための活動を開始している。しかし、今のところ、行動の変化をもたらす必要があると認識するところで留まっている。

・官民共同の「サイバーセキュリティハブ」は、情報を共有することによって、脅威を認識し管理することを助け、重要な役割を果たしている。

・安全なオンラインを確保し、脅威に対する認識を高め、消費者や、中小企業に助言を与える必要がある。一方、我々は、まだ機能していないビジネスに対する他の手段が必要であり、その他の要求にも対応する必要がある。我々は、デジタルチャネルやオンラインメディアを用いて、信用や資産に対する脅威についての認識を高め、オンラインによる指導を含めた、中小企業のサイバーを認識した行動を推奨する。

・ビジネスの重要な情報や資産の防御を改善するために、政府は、サイバーセキュリティの侵害についての分析や情報の透明性を高めることが重要と考えている。BIS（Department for Business, Innovation and Skills：英国知的財産庁）は、2013 年に、「サイバーセキュリティの侵害に関する包括的調査結果」を公表する予定である。

・個人の消費者向けと同様に、小規模ビジネスに対してセキィリティ製品の市場を導くのは困難である。そこで、BIS は、顧客が良いセキュリティ製品やサービスを選別することの助けとなる、産業界による基準やガイダンスの発展を推進する。BIS はまた、産業界によるサイバーセキュリティについての企業の仕事ぶりについての水準が、より一般に市場における差別化要因として利用される方法を模索する。BIS は、利用者、産業界、品質保全機関（国内、欧州、国際）と協働して、適切な基準の開発を促進する。

・ビジネスサービスの供給者は、関心を引き上げることにおいて重要な役割を果たす。BIS は、自身の活動として、実業界にサイバーセキュリティに関するメッセージを送る一方で、ビジネスサービスの専門家や保険市場とともに、どうしたら我々が、サイバーセキュリティがビジネスリスクとして効率的に管理できることを確信できるかということについて協働する。BIS は、専門的なビジネスサービスの供給者（保険会社、弁護士、監査法人などを含む）と戦略的な会議を開催し、どのようにしたらこれらの供給者が、リ

スクを管理し減少させる助けとなるものとして、事業者に提供するサービスを開発できるのかについて話し合う。

・政府は小売事業者と、小売業に存在する脅威を伝えるために特別な活動を行う。英国は、世界でも大きなオンライン経済が発達している国の一つで、2009 年の取引高は 1000 億ポンド以上と推定される。英国の小売店は、他の先進国よりもオンラインで販売する割合が高い。

この繁栄しているオンライン小売部門を防御するために、政府は、効果的な報告や情報共有を含む、この部門に特別重要な課題に対処するための「小売業サイバーセキュリティフォーラム」を設立しつつある。政府は、消費者が、安全なオンラインを利用できるように、英国小売業機構やその会員と協働していく。

・顧客との関係を通して、インターネットサービスプロバイダーは、英国におけるサイバー攻撃を識別し、防御することにおいて、重要な役割を果たしている。政府との間の既存の関係に加えて、我々は、自主的に適用されるいくつかの指導原理を協働して策定していく。これらの指導原理には、中小企業のために、インターネット利用者が自身のシステムにおける悪意のある行為に対応することを補佐したり、政府と中小企業の間で脅威に関する情報を交換したり、脅威を認識する共同の手段を構築することや、中小企業が顧客に顧客のコンピューターから情報漏えいがあった場合にそれを伝えたり、サイバー攻撃から顧客を防御することに関する取り決めなども含まれる。

“ビジネスの機会の育成”

・サイバー空間がもたらす機会を民間部門が享受することを助成するために、我々は、国際的な範囲で、英国に、活発で革新的なサイバーセキュリティ部門を育成することを目指している。

・GCHQ（政府通信本部）は、サイバーセキュリティにおける国際クラスの専門知識の本拠地である。政府は、政府機構の中核的なセキュリティや防諜活動を損なうことなく、専門家が、経済成長をより直接的に供与できたり、英国のサイバーセキュリティ部門の発展を手助けできる方法を模索する。

・我々は、公共サービスネットワークに納入される ITC 製品に対して、より高い水準のサイバーセキュリティを要求する。中小企業も、新たな概念や改革の推進の一翼を担えるように、我々は、成長の見直しの一環として、中小企業が政府の入札に参加できることについて提案を行う。政府は、入札を分割するか、あるいは大企業に対する契約に下請け契約を内包させることによって、政府のサイバーセキュリティ関係の仕事の少なくとも 25%が中小企業に行くことを期待している。内閣府は各官庁とともに、中小企業との全ての新たな契約において透明性が保持されていることを確実にする。

・我々はまた、機密性の高い軍装備の供給者に対するサイバーセキュリティの水準を引き上げる予定である。我々はこれを国家安全保障の観点から行う。例えば、装備の性能に

関する重要なデータが、装備が実践に配備される前に外国の情報機関によって盗まれることを防ぐものである。政府は、公共調達の水準の向上が、英国のサイバーセキュリティ市場を前進させることを望んでいる。

・問題の度合いについてのより良いデータや、発展していく保険市場、良いサイバーセキュリティとはどんなものであるかということについてのより明瞭な指標は、相互に、英国内の需要を後退させる要因を取り除くものとなりうる。UKTI（貿易産業省）は、保険分野の貿易協会と、これらの増大する国内の強みが英国企業の海外での販売を強化することにつながるように協働している。我々は脅威を機会に置き換え、サイバーセキュリティを全ての英国のビジネスにとって前向きなものとし、英国の競争力のある利点としていく。

以上