第5節 サイバー空間をめぐる動向

1 サイバー空間と安全保障

近年の情報通信技術（ICT）の発展により、インターネットなどの情報通信ネットワーク（Information and Communications Technology）は人々の生活のあらゆる側面において必要不可欠なものになっている。一方、重要インフラの情報通信ネットワークに対するサイバー攻撃[1]は、人々の生活に深刻な影響をもたらしうるものである。

サイバー攻撃の種類としては、情報通信ネットワークへの不正アクセスやメール送信などを通じたウィルスの送り込みによる機能妨害や情報の改ざん・窃取、大量のデータの同時送信による情報通信ネットワークの機能阻害などがあげられるが、インターネット関連技術は日進月歩であり、サイバー攻撃[2]も日に日に高度化、巧妙化している。

軍隊にとって情報通信は、指揮中枢から末端部隊に至る指揮統制のための基盤であり、ICTの発展によって情報通信ネットワークへの軍隊の依存度が一層増大している。また、軍隊は任務遂行上、電力をはじめとする様々な社会インフラに依存しており、当該社会インフラに対するサイバー攻撃が、任務の大きな阻害要因になり得る。そのため、サイバー攻撃は敵の軍隊の弱点につけこんで、敵の強みを低減できる非対称的な戦略として位置づけられつつあり、多くの外国軍隊がサイバー空間における攻撃能力を開発しているとされている。また、国家等に害を加えようと意図する主体は、物理的な手法によって直接攻撃するよりもサイバー空間を通じた攻撃を選択する方がより容易である場合が多いと認識している[3]。さらに、情報収集目的のために他国の情報通信ネットワークへの侵入が行われているとの指摘があり、より多くの機微な情報がサイバー空間に保管されるようになるにつれ、こうしたサイバー攻撃による情報窃取の被害はより重大なものとなってきている。

こうしたことから、今やサイバーセキュリティは、各国にとっての安全保障上の重要な課題の一つとなっている。

2 サイバー空間における脅威の動向

このような状況のもと、諸外国の政府機関や軍隊などの情報通信ネットワークに対するサイバー攻撃が多発している[4]。

これらの一部については、中国の人民解放軍[5]、情報機関、治安機関、民間ハッカー集団や企業など様々な組織の関与が指摘[6]されている。また、

1 サイバー攻撃の標的には、大きくは国家間などの地球規模のほか、国や政府機関、地域社会、経済界やインフラ、企業、個人まで様々なものがある。そのためサイバー攻撃への対策は、それぞれの規模に対して最適な対策が必要であると言われている。

2 12（平成24）年9月、「防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて」では、サイバー攻撃の特徴として①多様性：実行者、手法、目的、状況などが多様であること、②匿名性：実行者の隠蔽（なりすまし）・偽装が容易であること、③隠密性：攻撃の存在を察知し難いものや、被害発生の認識すら困難であること、④攻撃側の優位性：手法によっては攻撃手段の入手が容易であることや、ソフトウェアのぜい弱性を完全に排除することが困難であること、⑤抑止の困難性：報復攻撃や防御側の対策による抑止効果が小さいことなどがあげられている。

3 16（平成28）年2月、オバマ大統領が発表した「サイバー安全保障国家行動計画」による。

4 米行政予算管理局による連邦情報保証管理法に関する議会への年次報告書（15（平成27）年2月27日）によると、米国コンピューター緊急対処チーム（US-CERT：The United States Computer Emergency Readiness Team）は、14（同26）会計年度の米国政府に対するサイバー攻撃件数が69,851件発生したほか、US-CERTに報告されたサイバー攻撃の件数が政府機関・企業などを含め合計640,222件にのぼるとしている。また、16（同28）年2月の米国家情報長官「世界脅威評価」は、サイバー空間に対する脅威の主体としてロシア、中国、イラン、北朝鮮及び非国家主体を挙げ、例えば、①ロシアは重要インフラのシステムを標的としたサイバー攻撃や情報窃取など、より攻撃的なサイバー作戦の態勢を取っている、②中国は、米国政府、同盟国及び企業などに対する情報窃取を続けており、国内の安定や体制の正当性を脅かすと見なす標的にはサイバー攻撃を実施している、③北朝鮮は、おそらく政治目標の達成を支援するために、妨害や破壊を伴うサイバー攻撃を実施する能力及び意思を有している、④イランは、安全保障上の課題に対処し、情勢に影響を与え、また脅威に対処するため、情報窃取、宣伝活動、サイバー攻撃を実施している、⑤ISILは「ローン・ウルフ型」の攻撃を喚起するための新たな戦術として、米軍の軍人に関する機微な情報を標的とし公開した、などの見解を示している。ISILによるサイバー空間の利用については、Ⅰ部3章1節を参照。

5 13（平成25）年2月の米国情報セキュリティ企業「マンディアント」の「APT1：中国のサイバー諜報部隊の1つを暴露する」は、米国などに対する最も活動的なサイバー攻撃集団は、中国人民解放軍総参謀部第3部（当時）隷下の「61398部隊」であると結論づけている。またサイバー部隊である総参謀部第3部（当時）は、13万人の規模であるとの指摘がある。

6 米中経済安全保障再検討委員会の年次報告書（15（平成27）年11月）は、中国政府が大規模なサイバー諜報を支援しており、民間企業や米国政府などから情報を盗んだとしている。また、中国は宇宙やサイバー空間を戦略的に要となる分野として、攻撃的な能力の獲得を追求しているとし、また、サイバー戦能力によって、軍事的に優れた相手に対抗できるとみていると指摘している。

15（平成27）年5月に発表された中国の国防白書「中国の軍事戦略」[7]によれば、中国はサイバー戦力の建設を加速させるとしている。さらに、同年12月末、中国における軍改革[8]の一環として創設された「戦略支援部隊」の下にサイバー戦部隊が編成されたとの指摘もある。14（同26）年5月、米国司法省は、米国企業にサイバー攻撃を行ったとして、中国人民解放軍のサイバー攻撃部隊「61398部隊」の将校らを起訴したと発表した[9]。15（同27）年6月には、米国連邦人事管理局がサイバー攻撃を受け、米連邦職員や米軍軍人などのおよそ2,200万人分の個人情報が窃取されていたことが判明した。これらの攻撃にも中国が関与しているとの指摘[10]があるが、中国は政府の関与を否定し、中国人ハッカーによる「犯罪」だったと説明している。このほか、14年（同26）年7月、カナダ政府は中国からサイバー攻撃を受けたとして、中国を初めて名指ししている[11]。こうしたサイバー攻撃の背景にある中国の意図については、経済的に勝利することを目的とした国家戦略の一部として、中国軍及び諜報機関が米国などの企業から情報を窃取し、それらを自国企業にフィードバックしているとの指摘がなされている[12]。

14（同26）年10月、ホワイトハウスの非秘密情報システムが、ハッカーに侵入された[13]ほか、15（同27）年12月には、ウクライナで大規模な停電が発生した[14]。これらの攻撃については、ロシアの関与が指摘されている。ロシアについては、軍や情報機関、治安機関などがサイバー攻撃に関与しているとの指摘があり[15]、また、軍による独自のサイバー部隊が創設中とみられ、同部隊は敵の指揮・統制システムへのマルウェア（破壊工作プログラム）の挿入を含む攻撃的なサイバー活動を担うとされている[16]。こうした、ロシアによる活動の背景には、①ウクライナやシリアの問題についてのロシアの意志決定を支援するための情報収集、②軍事・政治的目的を支援するための工作、③将来の有事に備えたサイバー空間の環境整備の継続などの目標があると指摘されている[17]。

13（同25）年3月には、韓国の放送局、金融機関などに対するサイバー攻撃が、また、同年6月から7月にかけて、韓国大統領府、政府機関、放送局、新聞社などに対するサイバー攻撃が発生したほか、ソウル地下鉄へのサイバー攻撃も伝えられている。これらの事案について韓国政府は、過去の北朝鮮によるサイバー攻撃の手口と一致したとしている[18]。さらに、14（同26）年11月から12月にかけて、米国の映画会社に対するサイバー攻撃が発生した。米連邦捜査局（FBI）は同年12

Federal Bureau of Investigation

7 同国防白書では、「サイバー空間は、経済・社会発展の新たな支柱であり、国の安全保障の新分野である」、「サイバー空間における国際間の戦略競争は日増しに激化しており、多くの国がサイバー空間における軍事力を発展させている」、さらに、「中国はハッカー攻撃の最大の被害国の一つである」などの指摘がなされている。

8 15（平成27）年9月以降、中国は軍改革に関する一連の決定を公表しており、16（同28）年1月には戦略支援部隊などの新設が発表された。同部隊の任務や組織の細部は公表されていないものの、宇宙・サイバー・電子戦を担当しているとの指摘がある。

9 14(平成26)年5月19日、コメイFBI長官は、「中国政府が長い間、中国国営企業の経済的優位を得るために、サイバー攻撃を利用してきた」旨発言している。また同日、中国外交部報道官は「米国が事実をねつ造した」と発表し、米中戦略・経済対話の枠組みのもとに設置されている、サイバー作業部会の活動を停止させるとした。

10 米中経済安全保障再検討委員会の年次報告書（15（平成27）年11月）による。この他にも、米国連邦人事管理局（OPM：Office of Personnel Management）と同じ手口で、米国の航空会社への攻撃が行なわれたとしている。

11 14（平成26）年7月、カナダ政府発表による。

12 15（平成27）年6月の米中経済安全保障再検討委員会によるデニス・F・ポインデクスター氏へのヒアリングの際の発言による。また、米中経済安全保障再検討委員会の年次報告書（15（同27）年11月）は、先進装備、次世代情報技術、新素材及び生物技術などといった、中国の戦略的新興産業の技術分野が、中国のハッカー活動の関心対象となっているとの見方を指摘している。

13 14（平成26）年10月の米ワシントンポスト紙は、ロシア政府の関与が疑われるハッカー集団からのサイバー攻撃だったと報じた。

14 16（平成28）年2月の米ニューヨークタイムズ紙は、クリミア併合などで対立するロシア軍関与の疑いがあると報じた。

15 04（平成16）年11月、米ダートマス大学セキュリティ技術研究所（現セキュリティ技術社会研究所）の報告書「サイバー戦：各国における方法と動機についての分析」では、ロシアによるサイバー攻撃への軍、情報機関、治安機関などの関与を指摘している。

16 15（平成27）年9月、クラッパー米国家情報長官が下院情報委員会で「世界のサイバー脅威」について行った書面証言による。

17 米国家情報長官世界脅威評価（16（平成28）年2月）による。

18 韓国未来創造科学部（科学技術政策と情報通信技術（ICT）に関する事務を所掌する中央行政機関。13（平成25）年3月、教育科学技術部の科学技術関連業務と放送通信委員会及び知識経済部の一部業務を移管して設置）報道資料（13（同25）年4月及び7月）において、官・民・軍合同対応チーム（未来創造科学部、国防部、国家情報院、国内セキュリティ企業など18機関で構成）の調査結果として公表されている。

月、このサイバー攻撃は北朝鮮政府に責任があると判断するのに十分な証拠があると発表した[19]。北朝鮮については、このようなサイバー攻撃への政府機関などの関与[20]のほか、国家規模で人材育成を行っているとの指摘もある[21]。こうしたサイバー攻撃は、政治的な目的のために行われているとみられている[22]。

10（同22）年6月、「スタックスネット」と呼ばれる、産業制御システム（ICS）への攻撃を企図したマルウェアが発見され、その後もたびたび高度なマルウェアが発見されている[23]。

Industrial Control System

政府や軍隊の情報通信ネットワーク及び重要インフラに対するサイバー攻撃[24]は、国家の安全保障に重大な影響を及ぼし得るものであり、政府機関の関与も指摘されていることから、サイバー空間における脅威の動向を引き続き注視していく必要がある。

なお、わが国においても、15（同27）年5月には、日本年金機構がサイバー攻撃を受け、年金の受給者と加入者の個人情報が流出した。そのほかにも、ハッカー集団などから、政府機関や企業へのサイバー攻撃が行われている。

これらの他にも、意図的に不正改造されたプログラムが埋め込まれた製品が企業から納入されるなどのサプライチェーンリスクも指摘されている[25]ほか、家電製品などに組み込まれた「スマート」機器などインターネットに接続する機器の増加によって、ネットワークの複雑性が増大する可能性や、人工知能を搭載したシステムに対する誤作動を目的とした悪意のある攻撃が行われるなど、民間のインフラや政府システムの脆弱性が拡大する可能性があるとの指摘[26]もなされている。

3　サイバー攻撃に対する取組

こうしたサイバー空間における脅威の増大を受け、各国において、政府全体レベル及び国防省を含む関係省庁レベルなどで、各種の取組が進められている[27]。

近年新たな安全保障上の問題となっているサイバー攻撃に関しては、効果的な対応を可能とするうえで整理すべき論点が指摘されている。例えば、サイバー空間に関しては、国際法の適用のあり方等、基本的な点についても国際社会の意見の隔たりがあるとされ、米国や欧州、わが国などは、自由なサイバー空間の維持を訴え、ロシアや中国、新興国などの多くは、サイバー空間の国家管理の

19　FBIはその証拠として次の3点を指摘。①サイバー攻撃に使われたマルウェア（破壊工作プログラム）は、北朝鮮関係者が以前利用していたものと酷似していた。②データを消去したマルウェアには、北朝鮮のIPアドレス（インターネット上の住所）が組み込まれていた。③今回攻撃に利用されたツールは、13（平成25）年3月に北朝鮮が、韓国の放送局や金融機関にサイバー攻撃したものと類似性があった。

20　13（平成25）年11月、韓国報道各社が、韓国国家情報院が国会情報委員会の国政監査で北朝鮮のサイバー戦能力などについて明らかにしたと報じるとともに、北朝鮮の金正恩第1書記が、「サイバー戦は、核、ミサイルと並ぶ万能の宝剣である」と述べたと伝えた。また、16（同28）年2月に米国防省が公表した「2015年北朝鮮の軍事及び安全保障の進展に関する年次報告書」では、北朝鮮は攻撃的なサイバー作戦能力を保有しているとしている。さらに、15（同27）年1月、韓国の「2014国防白書」は、北朝鮮はサイバー部隊を集中的に増強し、規模は約6,000人と指摘している。

21　例えば、11（平成23）年6月の韓国の脱北者団体「NK知識人連帯」主催「2011北朝鮮のサイバーテロ関連緊急セミナー」における「北朝鮮のサイバーテロ能力」と題した発表資料は、北朝鮮のサイバー関連組織について、政府機関などの関与を指摘し、サイバー戦力養成のため、全国から優秀な人材を発掘し、専門教育を行っている、としている。

22　15（平成27）年9月、クラッパー米国家情報長官の下院情報委員会で「世界のサイバー脅威」について行った書面証言による。

23　特定のソフトウェアとハードウェアが組み込まれた制御システムを標的にするという点では確認されたものとして初のウィルス・プログラムであり、検知されることなく標的のシステムにアクセスし、情報の窃取やシステムの改変を実行する能力を有すると指摘されている。また、11（平成23）年10月に、「デューク」、12（同24）年5月「フレイム」、同年6月「ガウス」、同年8月「シャムーン」と呼称されるマルウェアの発見が伝えられている。

24　ウクライナの親ロシア派集団「サイバー・ベルクート」は14（平成26）年3月、NATOの複数のウェブサイトへのサイバー攻撃を行い、15（同27）年1月、ドイツ政府やドイツ連邦議会のウェブサイトへもサイバー攻撃を行った。また、同年6月、「シリア電子軍」は、米国防総省の陸軍のホームページを攻撃し不正アクセスを行った。さらに、国際ハッカー集団「アノニマス」は同年11月、パリ同時テロをめぐり、ISILに関連するアカウントを攻撃したと発表した。このように、ハッカー集団によるサイバー攻撃も多発している。

25　12（平成24）年10月、米下院情報特別委員会による「中国通信機器企業華為技術及び中興通訊が米国国家安全保障に及ぼす問題」と題する調査報告書では、米国重要インフラに対するサイバー攻撃能力や企図に対する懸念や、中国主要IT企業と中央政府、共産党、人民解放軍との不透明な関係がサプライチェーンリスクを増大させることへの強い懸念といった、国家安全保障上の脅威を理由に、中国大手通信機器メーカー「華為技術」及び「中興通訊」の製品を利用しないように勧告された。フランス、オーストラリア、カナダ、インド及び台湾などでも同様の動きがみられ、英国及び韓国などでは注意を促す動きがみられる。

26　16（平成28）年2月、米国家情報長官「世界脅威評価」による。

27　一般的に政府全体レベルでは、①サイバーセキュリティ関連部門の統合や運用部門の一元化、②専任のポストの設置や研究部門の新設及び拡充などによる政策部門及び研究部門の強化、③サイバー攻撃対処における情報機関の役割の拡大、④国際協力の重視、などの傾向があると考えられる。国防省レベルにおいても、サイバー空間における軍の作戦を統括する機関を新設するなど、サイバー攻撃への取組を国防戦略の中の重要な戦略目標と位置づけるなどの対応が進められている。

強化を訴えているなど、各国の主張は対立しているとの指摘もある。こうした状況を背景に、国際社会においては、サイバー空間における法の支配の促進を目指す動きがあり、15（平成27）年8月、国連の政府専門家会合は、サイバー空間を利用した行為に対する国際法の適用のあり方や、自発的かつ拘束力を有さない国家の行動規範等についての提言を含む報告書を発表している[28]。

参照》Ⅲ部1章2節7項（サイバー空間における対応）

1 米国

11（同23）年5月に発表された「サイバー空間のための国際戦略」は、サイバー空間の将来に関する米国のビジョンを提示し、その実現に向けて各国政府及び国民と協力するためのアジェンダを設定した。また、優先的に取り組むべき七つの政策分野として、経済、ネットワーク防護、法執行、軍事、インターネット・ガバナンス、国際的な能力構築及びインターネットの自由をあげている。

米国では、連邦政府のネットワークや重要インフラのサイバー防護に関しては、国土安全保障省が責任を有しており、同省のサイバー・セキュリティ・通信室（CS&C）が政府機関のネットワーク防御に取り組んでいる。
Office of Cybersecurity and Communications

米国は15年（同27）年2月に公表した「国家安全保障戦略」（NSS）において、今日の主要な脅威の一つとしてサイバー攻撃の脅威をあげている。
National Security Strategy
国防省の取組としては、14（同26）年3月に公表された「4年ごとの国防計画の見直し」（QDR）において、米国の国益に対するリスクであるサイバーの脅威は、個人、組織、国家といった様々な
Quadrennial Defense Review
主体により構成されており、国防省や産業ネットワーク・インフラへの不正アクセスによって、米国と同盟国・友好国の重要インフラが脅威にさらされているとの認識を示したうえで、米軍のサイバー戦能力を本土防衛上保持すべき重要な分野と位置づけ、引き続き、人材確保・育成及びサイバー任務部隊の拡充を行うとしている。

15（同27）年4月に公表された「米国防省サイバー戦略」は、サイバー脅威について、国家主体[29]及び非国家主体が米国のネットワークに対する破壊的なサイバー攻撃や米国の軍事技術情報の窃取などを企図しており、米国は深刻なサイバー脅威にさらされているとの認識を示している。そこで、国防省は、①国防省のネットワーク、システム及び情報の防護、②サイバー攻撃による深刻な結果からの米国及びその権益の防護、③軍事作戦の支援のための統合的なサイバー能力の提供、の3つをサイバー空間における主要な任務[30]とし、当該サイバー能力には、敵国軍事システムの破壊を目的としたサイバー作戦が含まれるとしている。

組織面では、戦略軍隷下のサイバーコマンドが、陸海空海兵隊の各サイバー部隊を統括し、サイバー空間における作戦を統括する。また、任務の拡充にともなってその組織を拡充し、国防省の情報環境を運用・防衛する「サイバー防衛部隊」を既に保有していることに加え、国家レベルの脅威から米国の防衛を支援する「サイバー国家任務部隊」、統合軍が行う作戦をサイバー面から支援する「サイバー戦闘任務部隊」を創設し、これら三部隊を「サイバー任務部隊」[31]と総称している。

16（同28）年2月、オバマ大統領は、「サイバー安全保障国家行動計画」を発表するとともに、

28 国連のサイバー問題に関する政府専門家会合は、日本、米国、ロシア、中国など計15か国（14（平成26）年7月の会合より計20か国）の専門家が参加し、04（同16）年から協議を続けている。15（同27）年8月に発表した報告書においては、国家によるICTの利用に対する国際法の適用について、①ICTの利用における国家主権等の諸原則の遵守、②国家が国際法に従って、かつ、国連憲章で認められた形でとり得る「固有の権利」への留意、③ICTを利用した国際違法行為を行うために国家が代理主体を使用することの禁止、④自国領域が非国家主体によってそのような行為を行うために使用されないことを確保すべき事等の見解が示された。また、国家の自発的な行動規範についても、重要インフラに対して故意に損害を与えるようなICT活動を実施又は支援すべきでない等の提言がなされた。

29 米国防省サイバー戦略では、ロシアや中国は先進的なサイバー能力及び戦略を獲得しているとした上で、ロシアの活動は秘密裏に行われており、その意図を読み取ることが難しいとしている。また中国は、知的財産を窃取し、中国企業に利益を与えているとしている。さらに、イラン及び北朝鮮のサイバー能力は高くないものの、米国及び米国の権益に対する敵対的な意図を公然と示しているとしている。

30 米国防省はサイバー空間における任務を遂行するために、①サイバー作戦実施のための即応的な部隊及び能力の構築・維持、②国防省の情報ネットワーク及びデータの防護並びに任務上のリスクの軽減、③関係省庁・企業などとの連携を通じた重大なサイバー攻撃からの米国及びその権益の防護体制の構築、④紛争管理におけるサイバー空間における各種手段の活用、⑤同盟国及びパートナー国との緊密な協力関係の構築、という五つの戦略構想を示している。

31 15（平成27）年4月、上院軍事委員会における米サイバーコマンド司令官の発言などによれば、三部隊には複数のチームが所属しているとされ、現在数十チームが活動中としている。また、州兵や予備役を活用し、18（同30）年9月までに133チーム（サイバー国家任務部隊（13チーム）、サイバー防衛部隊（68チーム）、サイバー戦闘任務部隊（27チーム）、支援チーム（25チーム））、6,200人規模にするとしている。

2017会計年度の予算要求において、サイバー安全保障に関する投資関連予算は最も重要な国家安全保障上の課題の一つと位置づけ、大幅に増加させることを発表[32]した。「サイバー安全保障国家行動計画」によれば、連邦政府全体の取組として、国家サイバー安全保障強化委員会の設置など、連邦政府におけるサイバー関連の技術、教育、人材登用などへの追加的な投資を行うこととしている。

国防省においても、2017会計年度の予算要求において、2016会計年度予算から15.5パーセントの増加となる67億ドルを計上している。サイバー任務部隊の編成の継続などサイバーコマンドの態勢整備のための予算を含むほか、防御的サイバー作戦能力[33]及び攻撃的サイバー作戦能力[34]の向上のための予算も計上している。

米国は、中国によるサイバー窃取は、国家安全保障に関する情報から機微な経済情報、米国の知的財産に至るまで、幅広く米国の利益を標的とし続けていると認識している。

15（同27）年9月、オバマ米大統領と習近平中国国家主席は首脳会談において、両国が知的財産のサイバー窃取を行わないことで合意[35]した。また、同年12月、米中両政府は、初のサイバー問題に関する閣僚級対話を実施し、「サイバー犯罪に対処するガイドライン」の策定、机上演習の実施、ホットラインの設置などに合意した。

2 NATO

11（同23）年6月に採択したサイバー防衛に関する北大西洋条約機構（NATO）の新政策及び行動計画は、①サイバー攻撃に対するNATOの政治的及び運用上の対応メカニズムを明確化し、②NATOが、加盟国によるサイバー防衛構築の支援や、加盟国がサイバー攻撃を受けた場合の支援を実施することを明確にし、③パートナー国などと協力していくとの原則を定めている。また、14（同26）年9月、NATO首脳会議において、加盟国に対するサイバー攻撃をNATOの集団防衛の対象と見なすことで合意している。

組織面では、北大西洋理事会（NAC）がNATOのサイバー防衛に関する政策と作戦の政治的監督を行っている。また、新規安全保障課題局（ESCD）がサイバー防衛に関して政策及び行動計画を策定している。さらに、NATOサイバー防衛センター（CCDCOE）がNATOのサイバー防衛に関する研究や訓練などを行う機関として認可されている[36]。

NATOは08（同20）年以降、サイバー防衛能力を高めるためのサイバー防衛演習を毎年行っている。

3 英国

英国では、11（同23）年11月に新たな「サイバーセキュリティ戦略」を公表し、15（同27）年までの目標を設定するとともに、能力強化、規範策定、諸外国との協力、人材育成など具体的な行動計画を規定した。15（同27）年11月には、「NSS・SDSR2015」を発表し、今後5年間で約19億ポンドをサイバー防衛能力向上のために投資し、サイバー空間における脅威を特定・分析する機能を強化することとしたほか、16（同28）年中に第2次国家サイバーセキュリティ戦略を発表するとした。

組織面では、政府全体のサイバーセキュリティ戦略の立案・調整などを行うサイバーセキュリティ・情報保証部（OCSIA）を内閣府のもとに、サイバー空間の監視などを行うサイバーセキュリ

32　2017会計年度の米大統領予算要求において、政府全体のサイバー安全保障関連予算は、総額約190億ドルを計上しており、これは2016年度予算から35パーセントの増加となる。
33　16（平成28）年3月、カーター米国防長官は、国防省のウェブページに対して民間のハッカーにあえてサイバー攻撃を仕掛けさせたうえで、セキュリティー上の弱点を検証する試験事業を同年4月から開始すると発表しており、国防省は、防御的サイバー能力の強化も図るための革新的な取組も行っている。
34　米軍は攻撃的サイバー能力を既に運用していることを明らかにしており、例えば、ISILに対し、指揮命令系統の分断を目的に、ネットワークに過剰な負荷をかけるなどしている。
35　首脳会談でオバマ米大統領は、中国のサイバー攻撃に非常に深刻な懸念を表明し、あらゆる可能な手段を行使すると経済制裁の適用を示唆したと伝えられている。その一方で、サイバー空間での犯罪の取り締まりに関する米中閣僚級対話の開催に合意した。
36　13（平成25）年6月、NATO国防相会合では、初めてサイバー防衛を主要議題とし、緊急対応チームを創設するとともに、同年10月までにサイバー防衛体制を完全に稼働させることで合意した。

ティ運用センター（CSOC：Cyber Security Operations Centre）を政府通信本部（GCHQ：Government Communications Headquarters）のもとに設置している。さらに、国防省においては、省内のサイバー活動を一元化する国防サイバー作戦グループ（DCOG：Defence Cyber Operations Group）を設置している[37]。同年11月に発表された「NSS・SDSR2015」では、サイバー攻撃に迅速かつ効果的に対応するために、サイバー攻撃に最初に対応する部隊であるGCHQのもとに国家サイバーセンターを設立するとしている。

また英国は、15（同27）年1月、キャメロン英首相とオバマ米大統領がサイバー防衛分野における協力強化[38]で一致した。さらに中国とは、知的財産などのサイバー窃取を実施・支援しないことで合意[39]するなど、各国との連携強化に努めている。

4 オーストラリア

オーストラリアは、13（同25）年1月、初の「国家安全保障戦略」を公表し、サイバー政策及び作戦の統合が国家安全保障上の最優先課題の一つであるとした。また、16（同28）年4月、20（同32）年までの新たな「サイバーセキュリティ戦略」を発表し、国民の安全の確保、民間企業によるサイバーセキュリティへの参画、脅威情報に関する情報共有等について規定した。

組織面では、政府内のサイバーセキュリティ能力を1カ所に集約した、オーストラリアサイバーセキュリティセンター（ACSC：Australian Cyber Security Center）が、14（同26）年11月に設置され、政府機関と重要インフラに関する重大なサイバーセキュリティ事案への対処を行っている[40]。また、ACSCは15（同27）年7月、初のサイバーセキュリティに関する報告書[41]を出し、オーストラリアに対するサイバー脅威の数、種類、強度がいずれも増加しているとしている。

また、16（同28）年2月に発表された国防白書では、サイバー攻撃は情報ネットワークに依存した豪軍の戦闘能力にとっての直接の脅威であるとして、国防省のサイバー戦力及びシステムを強化する方針を示している。

5 韓国

韓国では、11（同23）年8月に「国家サイバーセキュリティ・マスタープラン」が制定され、サイバー攻撃対処における国家情報院[42]の統括機能が明確化されたほか、予防、検知、対応[43]、制度及び基盤の五つの分野を重点的に推進することとされた。国防部門では、10（同22）年1月に、サイバー空間における作戦の計画、実施、訓練及び研究開発を行うサイバー司令部が設置され、現在では国防部直轄部隊として運用されている[44]。15（同27）年4月、韓国政府はサイバー攻撃対策を強化するため、大統領府の国家安全保障室にサイバー担当補佐官を新設した。

37 このほか、13（平成25）年9月、英国防省は、コンピュータの専門家数百人を同国のサイバー防衛の最前線で勤務する予備役として採用することを発表し、統合サイバー予備役の創設を認めた。
38 ホワイトハウスの発表によると、英国のGCHQと保安庁（SS：Security Service）、米国の国家安全保障局（NSA：National Security Agency）と連邦捜査局（FBI）がサイバーセキュリティとサイバー防衛に関して密接に協力するとした。さらに、15（平成27）年11月、米英両政府のサイバー、金融及び情報関連機関などが参加し、米英両国のサイバー協力及び金融業界におけるサイバー事案に対する効果的な対応能力を強化するために共同訓練を実施した。
39 15（平成27）年10月、習近平中国国家主席が国賓として英国を訪問。キャメロン英首相と首脳会談を行った。
40 ACSCは、豪州犯罪委員会、豪州連邦警察、豪州治安情報機関、豪州通信電子局、豪州コンピュータ緊急対処チーム及び国防情報機構の職員から構成され、サイバー空間における脅威分析や官民双方のインシデント対応を行っている。また、17（平成29）年までに約300名体制になるとしている。
41 同報告書によれば、豪州を狙うサイバー空間の敵には、①外国政府の支援を受けた敵、②重大かつ組織化された犯罪者、③特定の問題に動機づけられた集団や独自の不満を持つ個人がいるとしている。
42 国家情報院長のもとには、国家のサイバーセキュリティ体制の確立及び改善、関連政策及び機関間の役割調整、大統領の指示事項に関する措置や施策などの重要事項を審議する国家サイバーセキュリティ戦略会議が設置されている。
43 14（平成26）年2月、韓国国防部は、他国を攻撃するサイバー兵器の開発計画を国会で報告したと伝えられている。
44 12（平成24）年8月に国防部が大統領に提出した「国防改革基本計画」（2012～2030）においては、将来に向けた軍改革の一つとして、サイバー戦対応能力を大幅に拡充することがあげられている。