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のほか、電力システムなどの重要インフラへのシステムダウンや乗っ取りを目的とした攻撃などがあげられる。また、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重要インフラに依存しており、これらの重要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、国家など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]、

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・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、オバマ米大統領（当時）が発表した「サイバーセキュリティ国家行動計画」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米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み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。

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、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」のもとにサイバー戦部隊が編成されたとの指摘もある。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[9]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。また、中国はサイバー攻撃により、他国の軍の作戦計画や国家安全保障の意思決定のプロセス、重要インフラなどに関する機微な情報を得ているとの指摘[10]がなされている。さらに、最近、中国のサイバー攻撃に変化が見られ、多数の素人による攻撃から、少数精鋭かつ専門性の高い攻撃を実施する方向へと変化していると指摘[11]されている。

15（同27）年12月、ウクライナで大規模な停電が発生した[12]。この攻撃については、ロシアの関与が指摘されている。また、米国政府は、ロシア情報機関が16（同28）年の米大統領選挙の影響工作[13]のためサイバー攻撃[14]を行ったと批判した。そして、米司法省は17（同29）年3月、米大手インターネット企業から5億件以上の個人情報が流出したサイバー攻撃を実施したとして、ロシア連邦保安庁（FSB）の要員2名を含む4名のハッカーを起訴したと発表した。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される。また、軍による独自のサイバー部隊[15]の存在が明らかとなっている。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指摘されている[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]。

16（同28）年12月には、韓国軍内部ネットワークへのサイバー攻撃が行なわれていたことが判明した。韓国国防部によると、初めて軍内部の専用ネットワークがハッキングされ、このサイバー攻撃により、軍事秘密を含む一部の軍事資料が流出している。この事案について韓国軍サイバー軍司令官は、北朝鮮によるサイバー攻撃と推測される

6 米中経済安全保障再検討委員会の年次報告書（16（平成28）年11月）は、中国は国家安全部と軍の組織によるサイバー諜報に加え、中国の多数の非国家主体が米国を標的としたサイバー諜報を実施している。こうした主体には、政府と契約したハッカー、民間の「愛国ハッカー」、犯罪組織が含まれていると指摘している。

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 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われたとしている。

10 16（平成28）年11月、米中経済安全保障再検討委員会による年次報告書による。

11 16（平成28）年11月、米中経済安全保障再検討委員会による年次報告書による。

12 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。

13 17（平成29）年は、3月にオランダ総選挙（下院議会）、5月にフランス大統領選挙と欧州主要国で重要な選挙が実施され、同様のサイバー攻撃による影響工作が懸念された。フランスの大統領選挙期間中には、ロシアに対して強硬姿勢と評されるマクロン氏が、サイバー攻撃に加えて、租税回避地に隠し財産があるかのようなフェイクニュースを拡散される被害に遭ったとされる。同氏は大統領就任後、仏露大統領共同記者会見の場において、ロシアメディアを虚偽宣伝団体（organes de propagande mensongère）だと名指しで非難している。同年秋には、ドイツ連邦議会選挙が予定されており、同様の事案が引き続き懸念されている。

14 16（平成28）年10月、米国土安全保障省とクラッパー米国家情報長官による共同声明。また、同年12月、ロシアによる米国へのサイバー攻撃に関する米国土安全保障省及びFBIの共同報告書。及び、17（同29）年1月、米大統領選に対するロシアのサイバー攻撃に関する米情報コミュニティの報告書による。

15 17（平成29）年2月、ロシアのショイグ国防相の下院議員の説明会での発言による。発言によれば、ロシア軍に「情報作戦部隊」が存在すると明らかにされ、欧米との情報戦が起きているとし「政治宣伝活動に対抗するため」と強調、防衛目的との認識を示した。また、ロシアのサイバー軍の要員は約1，000人との指摘がある。

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。

と発言[18]している。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[19]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[20]。こうしたサイバー攻撃は、軍事的作戦として行われているとみられる。

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[21]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[22]。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[23]もなされている。また、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[24]。

Industrial Control System

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[25]。

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など、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[26]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、例えば15（平成

18 各種報道による。また、攻撃に使われたIPアドレス（インターネット上の住所）は中国の瀋陽とされ、過去に北朝鮮が関与したサイバー攻撃もこのIPアドレスが使われたと指摘されている。

19 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、17（同29）年1月、韓国の「2016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7,000人と指摘している。

20 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。

21 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。

22 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。

23 16（平成28）年2月、米国家情報長官「世界脅威評価」による。

24 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。

25 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。

26 情報の自由な流通や政府のみならず民間企業・市民社会を含むマルチステークホルダー・アプローチなどを訴えている。

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などについての提言を含む報告書を発表している[27]。

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[28]した。

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

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、任務の拡充に伴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「サイバー防護部隊」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。

17（同29）年1月に発足したトランプ政権は、発足初日に発表した米軍再建に関する政策の中で、サイバー戦の分野に関し、国家安全保障の秘密とシステムを保護するためにあらゆる手段を講じる必要があるとの認識を示した上で、米軍のサイバーコマンドにおいて防御的及び攻撃的なサイバー能力を発展させることを優先的課題とすることを明らかにした。

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（当時）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[32]したが、依然として中国からのサイバー諜報が続いていると指摘[33]されている。

---

27 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。

28 優先的に取り組むべき7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。

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5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）、サイバー防護部隊（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。

32 首脳会談でオバマ米大統領（当時）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。

33 16（平成28）年11月、米中経済安全保障再検討委員会による年次報告書による。

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は08（同20）年以降、NATO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。NATOとEUはサイバー安保・防衛分野での連携を拡大[34]するとしている。

また、08（同20）年には、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[35]され、エストニアの首都タリンに設置された。同センターは、サイバー活動と国際法の関係に関する研究などを行っており、「タリンマニュアル」[36]を作成するなどの活動を行っている。17（同29）年2月、同マニュアルの続編となる「タリンマニュアル2.0」が公表され、国家責任法、人権法、航空法、宇宙法、海洋法といった平時に関する法規範から、「武力の行使」や武力紛争法といった有事に関する法規範に至るまで、幅広い論点について検討が行われており、計154の「規則」に関する見解が述べられている。

③ 英国

英国は、15（同27）年11月に「NSS・SDSR 2015」において、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していくことを明らかにした。16（同28）年11月には、新たな「サイバーセキュリティ戦略」を公表し、英国がサイバーの脅威に対し安全かつデジタルの世界において繁栄するためのビジョンを提示した。このビジョンを達成するため、サイバー脅威に対し効果的に「防護」する手段の保持、攻撃的手段の保持による「抑止」、最先端技術の「開発」が必要としている。

政府全体のサイバーセキュリティ政策に関しては、戦略的方針を提示し、組織横断的な計画の調整などを行うサイバーセキュリティ・情報保証部（OCSIA）がある。16（同28）年10月には、国のサイバーインシデントに対応し、官民のパートナーシップを推進するため、国家サイバーセキュリティセンター（NCSC）が政府通信本部（GCHQ）の傘下機関として新しく創設された。

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などについて規定した。

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）が、14（同26）年11月に設置され、政府機関と重要インフラに

34 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。
35 16（平成28）年7月、NATO首脳会合に際し発出された「共同宣言」による。
36 「タリン・マニュアル」及び「タリン・マニュアル2.0」は、両文書ともに、NATOの公式見解ではなく、あくまでも同プロジェクトに参加したメンバー（米海軍大学のマイケル・シュミット教授がプロジェクトリーダーを務め、欧米等の実務家、国際法学者、サイバー技術専門家等が参加）による独立した成果物と位置づけられている。

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[37]。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[38]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[39]の統括機能が明確化されたほか、予防、検知、対応[40]、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[41]。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。さらに、国防部は、国防サイバー安保のビジョンと中長期の発展方向を提示した「国防サイバー安保戦略書」を作成しており、「国防サイバー危機対応実務マニュアル」を用意してサイバー危機への迅速な対応手順を定めている。合同参謀本部においては、15（同27）年にサイバー作戦総括部署を新設し、合同参謀本部議長にサイバー作戦に関する統制権限を付与して、「合同サイバー作戦」教範を発刊するなど、合同参謀本部を中心にサイバー作戦遂行体系を一元化している。

37 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。
38 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。
39 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。
40 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。
41 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。