打ち上げることに成功するなど、高い技術力を有している。なお、19（平成31）年3月、モディ首相は、低軌道上の人工衛星をミサイルで撃ち落とす実験に成功したと発表した。

組織面では、宇宙庁が宇宙開発政策を実行し、ロケットの開発、打ち上げ、衛星の開発、製造などを行うインド宇宙研究機関（ISRO）を管理している。
Indian Space Research Organization

6 韓国

韓国は、90年代後半から宇宙開発を本格化させたものとみられる。現在の宇宙開発は05（平成17）年に施行された「宇宙開発振興法」の下、文政権が発表した「第3次宇宙開発振興基本計画」に基づき推進されている。同計画は、40（令和22）年までのビジョンを提示し、①宇宙ロケット技術の自立、②人工衛星の活用サービスと開発の高度化、③宇宙探査の開始、④韓国型衛星航法システム（KPS）の構築などに重点をおいている。
Korean Positioning System

また、従来より韓国は、衛星の打ち上げを他国に依存してきたが、18（平成30）年11月、純国産ロケットとして開発中の「ヌリ号」の試験機打ち上げに成功したと発表した。

組織面では、韓国航空宇宙研究院が実施機関として研究開発を主導する。また、国防科学研究所が各種衛星の開発利用に関与している。

第3節 サイバー領域をめぐる動向

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おり、そのため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。
Information and Communications Technology

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、メール送信などを通じたウイルスの送り込みによる機能妨害、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妨害のほか、電力システムなどの重要インフラのシステムダウンや乗っ取りを目的とした攻撃などが挙げられる。また、インターネット関連技術は日進月歩であり、サイバー攻撃も日に日に高度化、巧妙化している[2]。

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を必要とする場合があり、これらの重要インフラに対するサイバー攻撃が、任務の大きな妨害要因になり得る。そのため、サイバー攻撃は敵の軍事活動を低コストで妨害可能な非対称的な攻撃手段として認識されており、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みられる。特に、中国及びロシアは、ネットワーク化された部隊の妨害やインフラの破壊などのために、軍のサイバー攻撃能力を強化していると指摘されている[3]。

また、国家などに害を加える意図を有する主体（非国家主体を含む）は、物理的な手法による直接攻撃よりも、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可能性が高い[4]。さらに、情報収集目的のために他

1 サイバー攻撃の標的には、大きくは国家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（いんぺい）・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挙げられている。
3 米国防情報長官「世界脅威評価書」（18（平成30）年3月）による。
4 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。

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、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一層重大なものとなってきている。

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おり[5]、中には、政府機関の関与が指摘されている事案も存在する。また、中国、ロシア、北朝鮮は軍としてサイバー攻撃能力を強化しているとみられる。

1 中国

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」[6]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ほか、同年12月末、中国における軍改革[7]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みられる。同部隊は17万5,000人規模とされ、このうち、サイバー攻撃部隊は3万人との指摘もあるなど、中国は軍のサイバー戦力を強化していると考えられる。

中国は、平素から機密情報の窃取を目的としたサイバー攻撃を行っているとされており[8]、例えば、以下の事案への関与が指摘されている。

・15（平成27）年6月、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[9]
・18（平成30）年1月及び2月、米海軍の契約業者が中国政府のハッカーによるハッキングを受け、潜水艦搭載の超音速対艦ミサイルに関する極秘情報が流出[10]
・18（平成30）年12月、米国などは、中国国家安全部と関連するサイバーグループ「APT10」が少なくとも12か国に対して知的財産などを標的とするサイバー攻撃を実施したと発表。米国は、「APT10」が、各国政府機関に対するサイバー攻撃を行ったほか、米企業から防衛や宇宙、航空、資源開発などの情報を盗んだと指摘

なお、わが国においても、「APT10」による民間企業、学術機関などを対象とした長期にわたる広範な攻撃が確認されている。

2 ロシア

ロシアについては、軍のサイバー部隊[11]の存在が明らかとなっており、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[12]。

5 米行政予算管理局が連邦情報セキュリティ管理法に基づき議会に報告している年次報告書によると、17米会計年度に連邦政府機関から報告されたサイバーセキュリティ・インシデントの件数は、3万5,277件。また、19（平成31）年1月の米国家情報長官「世界脅威評価書」は、米国に対して最も重大なサイバー脅威を与える主体として、中国、ロシア、イラン及び北朝鮮を挙げ、それぞれ、①中国は、米国の軍事の核となるシステム及び重要インフラのシステムに対する、サイバー諜報による継続的な脅威、及びサイバー攻撃によるより大きな脅威をもたらしている。②ロシアは、米国及びその同盟国に対し、サイバー諜報、サイバー攻撃及び影響工作による脅威をもたらしている。③イランは、サイバー諜報及びサイバー攻撃による脅威をもたらしている。④北朝鮮は、金融機関に重大な脅威を与え、引き続きサイバー諜報による脅威をもたらすとともに、妨害的なサイバー攻撃を実施する能力を有している、との見解を示している。

6 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」、「中国はハッカー攻撃の最大の被害国の一つである」などと指摘している。

7 戦略支援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。戦略支援部隊については、Ⅰ部2章2節を参照

8 18（平成30）年9月公表の「米国防省サイバー戦略」による。中国のサイバー攻撃については、人民解放軍、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を指摘している。さらに、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、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おり、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。

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 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。両国は知的財産のサイバー窃取を行わないことで合意しているが、依然として中国からのサイバー諜報が続いているとされる。

11 17（平成29）年2月、ロシアのショイグ国防相の下院の説明会での発言による。ロシア軍に「情報作戦部隊」が存在するとし、欧米との情報戦が起きており「政治宣伝活動に対抗する」として、防衛目的との認識を強調した。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。

12 15（平成27）年9月、クラッパー米国家情報長官（当時）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。

ロシアは、サイバーを用いた情報作戦により、民主主義プロセスに挑戦していると指摘されており[13]、例えば、以下の事案への関与が指摘されている。

・14（平成26）年、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。17（平成29）年3月、米国政府は、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[14]
Federal Security Service
・15（平成27）年12月、ウクライナで大規模な停電を発生させたサイバー攻撃が発生。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られた
・16（平成28）年の米大統領選挙の影響工作のためのサイバー攻撃[15]
・17（平成29）年6月、ウクライナを中心に各国でランサムウェア「NotPetya」によるサイバー攻撃が発生。18（平成30）年2月、米英両政府は、ロシア軍によるものと発表
・18（平成30）年10月、米英両政府は、世界アンチ・ドーピング機関、化学兵器禁止機関、米国民主党全国大会などに対する一連のサイバー攻撃事案についてロシア軍参謀本部情報総局によるものと発表

3 北朝鮮

北朝鮮については、当局で人材育成を行っており[16]、サイバー部隊を集中的に増強し、約6,800人を運用中と指摘されている[17]。

北朝鮮は、サイバー攻撃を用いた金銭窃取のほか、軍事機密情報の窃取や他国の重要インフラへの攻撃能力の開発を行っているとみられている。例えば、以下のサイバー攻撃への関与が指摘されている。

・16（平成28）年9月、韓国軍内部ネットワークへのサイバー攻撃が発生。17（平成29）年5月、韓国国防部は、北朝鮮ハッカー組織と推定される勢力によるものとの結論を下したと報じられた[18]。また、このサイバー攻撃により、韓国の軍事機密文書が流出したと指摘されている
・17（平成29）年5月、マルウェア「ワナクライ」により、世界150か国以上の病院、学校、企業などが保有する電子情報を暗号化し、使用不能にするサイバー攻撃が発生。我が国や米英政府などは、北朝鮮によるものであると発表[19]。また、このサイバー攻撃によって14万ドル分のビットコインが集められたとの指摘がある
・17（平成29）年9月、複数の米国電力会社にスピアフィッシング・メールによるサイバー攻撃が発生。同年10月に、米国情報セキュリティ企業「ファイアアイ」は、北朝鮮との関連が濃厚とされるサイバー脅威グループによって行われたと公表
・18年（平成30）年2月、韓国国家情報院は北朝鮮が仮想通貨を奪うために韓国の取引所などへのハッキングを繰り返しており、数百億ウォン（数十億円）相当を奪っていると報告したとされる
・19（平成31）年3月、国連安保理北朝鮮制裁委員会専門家パネル最終報告書は、17（平成29）年1月から18（平成30）年9月にかけて、北朝鮮がわが国を含むアジアの仮想通貨交換業者に対して少なくとも5回サイバー攻撃を行い、合計5億7,100万ドル（約630億円）を奪ったと

13 18（平成30）年9月公表の「米国防省サイバー戦略」による。
14 このインターネット企業からは、13（平成25）年にもサイバー攻撃を受けて約30億人分の情報が流出している。
15 16（平成28）年10月の米国土安全保障省と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（平成29）年1月の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。なお、17年（平成29）年のフランス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だと名指しで非難した。
16 17（平成29）年1月発刊の韓国の「2016国防白書」によると、北朝鮮のサイバー関連組織について、当局の関与を指摘し、サイバー戦力養成のため、全土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。
17 19（平成31）年1月発刊の韓国の「2018国防白書」による。また、13（平成25）年11月、北朝鮮の金正恩第1書記（当時）が、「サイバー戦能力は、核、ミサイルと並ぶ万能の宝剣である」と述べたと報じられている。
18 17（平成29）年5月の韓国・国防日報電子版による。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）の中の一部が、既存の北朝鮮ハッカーが使用していた中国・瀋陽地域のものと識別されたと指摘されている。
19 日本、米国、英国、豪州、カナダ、ニュージーランドが非難声明を発出。なお、JPCERT/CCによると、日本では600か所、2,000端末以上が感染したとされている。

指摘

4 その他の脅威の動向

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や、産業制御システムへの攻撃を企図した高度なマルウェアの存在も指摘されている。この点、米国議会は18（平成30）年8月、政府機関がファーウェイ（華為）などの中国の大手通信機器メーカーの製品を使用することを禁止する条項を盛り込んだ国防権限法を成立させた。また、中国の通信機器のリスクに関する情報を同盟国に伝え、不使用を呼びかけており、オーストラリアは、次世代通信規格「5G」の整備事業へのファーウェイとZTEの参入を禁止した。

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、また、近年、国家が関与するサイバー攻撃が増加しているとみられることから、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。

3 サイバー攻撃に対する取組

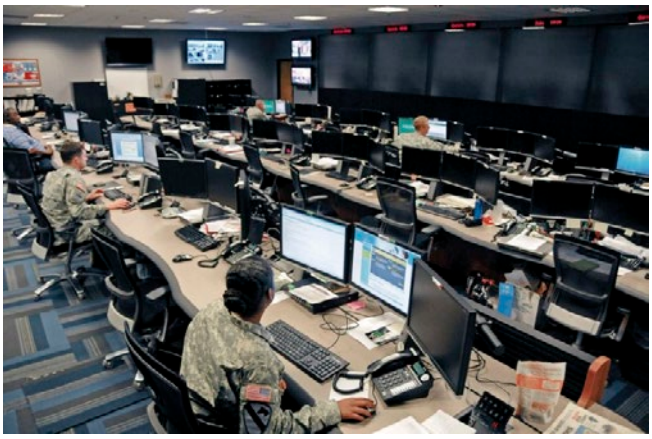
こうしたサイバー空間における脅威の増大を受け、各国において、各種の取組が進められている[20]。

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。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、例えば、米国や欧州、わが国などが自由なサイバー空間の維持を訴える一方、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。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、サイバー空間に関する国際会議[21]などの枠組みにおいて、国際的なルール作りなどに関する議論が行われている。

参照　Ⅲ部1章2節3項2（サイバー領域での対応）

1 米国

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）（Office of Cybersecurity and Communications）が政府機関のネットワーク防御に取り組んでいる[22]。



米陸軍サイバーコマンド
【Jane's by IHS Markit】

米国は、国家安全保障戦略（17（平成29）年12月）において、多くの国がサイバー能力を、影響力を行使する手段と捉えており、サイバー攻撃は現代戦の重要な特徴となっているとしたうえで、米国に対してサイバー攻撃を加えてくる相手を抑止、防御し、必要であれば打ち負かすとしている。そのため、米国は、①サイバー攻撃を特定し迅速に対応する能力の改善、②米国政府の財産、重要インフラ、情報などを守るためのサイバー手段及

20 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。

21 サイバー空間に関する国際会議は、11（平成23）年にヘーグ英外相（当時）が提唱して立ち上げ、一連の会議はロンドン・プロセスと称されている。100か国以上の政府、国際機関、民間セクター、NGOなどが一堂に会し、サイバー空間における諸課題に関する包括的な議論を行う、ハイレベルかつ最大規模の国際会議であり、直近では17（平成29）年11月に開催されている。

22 国土安全保障省は、18（平成30）年5月にサイバーセキュリティ戦略を発表。20（令和2）年までに200億台以上のデバイスがインターネットに接続されることが予想され、それによりリスクも高まるとしている。

び専門知識向上、③必要に応じて敵に対しサイバー作戦を実施するための政府の権限と手続きの改善などを図る方針を打ち出している。また、米国防省は、国家防衛戦略（18（平成30）年1月）において、サイバー防衛、抗たん性、運用全体へのサイバー能力の統合に投資していく方針を示している。さらに、米国防省サイバー戦略（18（平成30）年9月）においては、米国が中露との長期的な戦略的競争関係にあり、中露はサイバー空間における活動を通じて競争を拡大させ、米国や同盟国、パートナーへの戦略上のリスクになっていると指摘[23]したうえで、①サイバー軍の能力構築の加速、②悪意あるサイバー活動への対抗・抑止のための防衛、③同盟国及びパートナー国との協力促進といったアプローチが示されている。

19（平成31）年4月には、日米安全協議委員会（日米「2＋2」）が開催され、サイバー分野における協力を強化していくことで一致し、国際法がサイバー空間に適用されるとともに、一定の場合には、サイバー攻撃が日米安全保障条約にいう武力攻撃に当たり得ることを確認している。

米軍においては、18（平成30）年5月に統合軍に格上げされたサイバー軍が、サイバー空間における作戦を統括している。同軍は、陸海空海兵隊の各サイバー部隊並びに国防省の情報環境を運用・防衛する「サイバー防護部隊」、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」及び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」（これら三部隊を「サイバー任務部隊」[24]と総称。）などから構成されている[25]。

2 NATO

11（平成23）年6月に採択され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の政治上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（平成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みなすことで合意している。

組織面では、17（平成29）年11月に、サイバー作戦センターの新設及び加盟国が有するサイバー防衛能力のNATO任務・作戦への統合に関する方針に合意した。ベルギーに置かれた同センターは、23（令和5）年には全面稼働し、サイバー攻撃の能力を持つとの見通しが示されている。また、NATOは08（平成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ほか、EUとの間でもサイバー安保・防衛分野での連携を進展させている[26]。

研究や訓練などを行う機関としては、08（平成20）年、NATOサイバー防衛協力センター（CCDCOE）が認可[27]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」[28]を作成するなどの活動を行っている。17（平成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

23 「米国防省サイバー戦略」は、中国は米国の政府・民間機関から機密情報を窃取し、米国の軍事的優位や経済活力を減退させているとする一方、ロシアはサイバーを用いた情報作戦により米国民に影響を与え、民主主義プロセスに挑戦している、との認識を示している。

24 国防省によると、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。

25 戦略軍隷下であったサイバー軍は、18（平成30）年5月に統合軍に格上げされ、サイバー軍司令官は、他の統合軍司令官と同様、国防長官に対して直接報告を行うことが可能となった。米国防省は、サイバー軍の統合軍への格上げの発表に際して、サイバー空間は、陸・海・空の領域と同様に重要であり、サイバー空間での作戦能力は、軍事的成功にとって不可欠であるとし、今後、サイバー兵器、サイバー防衛、サイバー要員の規模・能力強化が課題との認識を示している。

26 16（平成28）年7月に、NATOとEUはサイバーセキュリティを含む、テロ・難民・移民問題などの新たな課題への対処における協力の拡大を目指した共同宣言に署名し、サイバー防衛に関する情報交換を行うなど協力を強化している。

27 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な課題とし、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安全に稼働させることで合意した。

28 「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、欧米などの実務家、国際法学者、サイバー技術専門家などが参加）による独立した成果物と位置づけられている。

といった平時に関する法規範から、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いる。

3 英国

英国は、15（平成27）年11月の「NSS・SDSR2015」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（平成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」する手段及び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。

組織面では、16（平成28）年10月に、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）を政府通信本部（GCHQ）に新設した。
National Cyber Security Centre
Government Communications Headquarters

4 オーストラリア

オーストラリアは、13（平成25）年1月の「国家安全保障戦略」において、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。16（平成28）年4月には、20（令和2）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）を設置し、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に対処している[29]。ACSCは15（平成27）年7月、初のサイバーセキュリティに関する報告書[30]を公表し、オーストラリアに対するサイバー脅威の数、種類、強度のいずれも増加しているとしている。また、17（平成29）年7月、国防省のサイバー戦能力及びシステム強化のため、軍にサイバー部隊を設立した[31]。
Australian Cyber Security Center

5 韓国

韓国は、11（平成23）年8月に「国家サイバーセキュリティ・マスタープラン」を制定し、サイバー攻撃対処における国家情報院[32]の統括機能を明確化したほか、予防、検知、対応[33]、制度及び基盤の五つの分野を重点的に推進するとした。国防部門では、国防部にサイバー対策技術チームを創設し、サイバー・ハッキング脅威に対応するとしているほか、「国防サイバー安保戦略書」や「国防サイバー危機対応実務マニュアル」に基づき、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（平成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。

29 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。
30 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。
31 17（平成29）年10月に発表された「国際サイバー・エンゲージメント戦略」によれば、軍事作戦を支援するための攻撃的なサイバー作戦は、通信電子局及び豪軍が協力して実施することとされている。
32 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。
33 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。